VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

SIP softwarový klient s podporou šifrování v prostředí Android

SIP Software Client with Encryption in an Android Environment

2013 Radek Mandrla

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Radek Mandrla**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: SIP softwarový klient s podporou šifrování v prostředí Android
SIP Software Client with Encryption in an Android Environment

Zásady pro vypracování:

V současné době se rozšiřuje nabídka chytrých telefonů s OS Android. Na této platformě existují volně dostupné SIP aplikace, které však z velké části nepodporují režim šifrování SIP signalizace (SIPS), či šifrování RTP (SRTP případně ZRTP). Cílem práce je proto vytvořit komplexní analýzu SIP VoIP klientů na platformě Android se zaměřením na podporu šifrování a na základě praktického testování vybrat nejvhodnější nástroj pro využití v praxi.
Body zadání:
1. Studijní část: bezpečnost VoIP na protokolu SIP, platforma Android.
2. Požadavky na SIP softwarového klienta z pohledu bezpečnosti.
3. Návrh vhodných SIP softwarových klientů s podporou šifrování pro hlubší analýzu.
4. Praktické testování vybraných SIP softwarových klientů se zaměřením na funkčnost šifrování.
5. Na základě výsledků definovat nejvhodnější SIP klient pro použití v praxi.
6. Teoretický návrh vylepšení bezpečnostních algoritmů u vybraného SIP softwarového klienta.

Seznam doporučené odborné literatury:

[1] SIP Security by Dorgham Sisalem, John Floroiu, Jiri Kuthan, Ulrich Abend, Henning Schulzrinne (May 26, 2009)
[2] Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions by David Endler and Mark Collier (Nov 28, 2006).
[3] Android Forensics: Investigation, Analysis and Mobile Security for Google Android by Andrew Hoog (Jun 29, 2011)
[4] Android Apps Security by Sheran Gunasekera (Feb 24, 2012)

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Filip Řezáč**

Datum zadání: 18.11.2011

Datum odevzdání: 07.05.2013

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně.

Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 12.4.2013

Podpis

Poděkování

Velmi rád bych poděkoval svému vedoucímu bakalářské práce Ing. Filipu Řezáčovi za pomoc při výběru tématu, sestavení obsahu a za rady, konzultace a připomínky, které mi byly cenným vodítkem při samotném vypracování. Také bych chtěl poděkovat své manželce a dětem za trpělivost.

Abstrakt

V současné době se rozšiřuje nabídka chytrých telefonů s operačním systémem Android. Na této platformě existují dostupné SIP aplikace, které však z velké části nepodporují režim šifrování SIP signalizace (SIPS), či šifrování RTP (SRTP případně ZRTP). Cílem bakalářské práce je proto vytvořit komplexní analýzu SIP VoIP klientů na platformě Android se zaměřením na podporu šifrování a na základě praktického testování vybrat nejvhodnější nástroj pro využití v praxi. V teoretické části je uveden základní princip VoIP komunikace a seznámení se s protokoly, které jsou nutné k provozu zabezpečené VoIP komunikace. V praktické části jsou popsány způsoby analýzy dostupných SIP softwarových klientů a jsou jednotlivě otestováni, zda skutečně podporují zabezpečenou VoIP komunikaci. V závěru je na základě výsledků definován nejvhodnější SIP softwarový klient pro použití v praxi.

Klíčová slova

Android, Asterisk, Autentizace, autorizace, důvěra, integrita, Man-in-the-middle, monitorování, RTP, SIP, SIP bezpečnost, SIP softwarový klient, SIP útoky, TLS, VoIP, Wireshark.

Abstract

Nowadays, the range of the smart phones with Android operating system is expanding dramatically. On this platform, the SIP applications are available, but mostly do not support the encryption mode of the SIP signalling (SIPS) or encryption of the RTP (SRTP or ZRTP). The main goal of my thesis is to create a comprehensive analysis of the SIP VoIP clients on the Android platform with focus on encryption support and according to the practical testing select the most convenient SIP client software for the practical application. The theoretical part of my thesis includes the basic principle of the VoIP communication and introduction of the proceedings that are required to operate a secure VoIP communication. In the practical part, there are described methods of analysis of the available SIP software clients and are individually tested whether they really support a secure VoIP communication. The conclusion of my thesis defines the most convenient SIP software client for the practical application, according to the gained results.

Key words

Android, Asterisk, Authentication, Authorization, Confidence, Integrity, Man-in-the-middle, Monitoring, RTP, SIP, SIP attack, SIP security, SIP software client, TLS, VoIP, Wireshark.

Seznam použitých symbolů a zkratek

AES	**(Advanced Encryption Standard)** – Symetrická šifra
DOS	**(Denial of Service)** – Odmítnutí služby
H.323	Signalizační protokol používaný ve VoIP
HMAC-SHA1	**(Keyed-Hash Message Authentication Code SHA1)** – Typ autentizačního kódu zprávy počítané s použitím kryptografické hashovací funkce (SHA1)
IAX	**(Inter-Asterisk eXchange)** – Protokol, kde signalizační a media data jsou přenášena jedním datovým tokem na jednotném portu
ISO/OSI	**(Open Systems Interconnection)** – Referenční model, jehož vrstvy jsou nezávislé a nahraditelné
MIKEY	**(Multimedia Internet KEYing)** – Protokol pro výměnu klíčů v reálném čase užívaný ve VoIP
MiTM	**(Man in The Middle)** – Způsob útoku snažící se zachytit data mezi komunikujícími stranami ve VoIP
QoS	**(Quality of Service)** – Zajištění vyhrazení dostupné přenosové kapacity
RTCP	**(RTP Control protokol)** – Řídící protokol pro RTP
RTP	**(Real-time Transport Protocol)** – Protokol přenosu v reálném čase
SAS	**(Short Authentication Strings)** – Využívá protokol ZRTP. Do SAS se se vkládá vypočítaný hash a účastníkovi se zašle protokolem ZRTP. Po doručení se spočítá hash a jestliže SAS obou účastníků neodpovídá, je zde riziko, že je konverzace odposlouchávána (MiTM)
SDES	**(Session Description Protocol Security Descriptions)** – Protokol pro výměnu klíčů v reálném čase užívaný ve VoIP
SDP	**(Session Description Protocol)** – Protokol k řízení multimediálního přenosu pro SIP
Self-signed Certificate	Certifikát podepsaný sám sebou
SIP	**(Session Initiation Protocol)** – Signalizační protokol používaný ve VoIP
SRTCP	**(Secure RTCP)** – Zabezpečený řídící protokol pro RTP
SRTP	**(Secure RTP)** – Zabezpečený protokol přenosu v reálném čase
SSH	**(Secure Shell)** – zabezpečený komunikační protokol
TCP	**(Transmission Control Protocol)** – Řídící přenosový protokol
TLS	**(Transport Layer Security)** – Protokol poskytující zabezpečenou komunikaci
UA	**(User Agent)** – Koncové zařízení v SIP infrastruktuře
UAC	**(User Agent Client)** – Koncové zařízení v SIP infrastruktuře, které generuje dotaz
UAS	**(User Agent Server)** – Koncové zařízení v SIP infrastruktuře, které vytváří odpovědi
UDP	**(Unified Datagram Protocol)** – Datagramový protokol používaný pro přenos v IP sítích
VoIP	**(Voice over Internet Protocol)** – Technologie pro přenos digitalizovaného hlasu pomocí paketů v počítačové síti
WebRTC	Protokol pro online komunikaci bez plug-inů v prohlížeči
ZRTP	**(Zimmermann RTP)** – Nádstavbový protokol pro SRTP

Seznam tabulek

Seznam obrázků

Obsah

1 Úvod

Voice over Internet Protocol je v dnešní době obecný název pro IP telefonii a ostatní internetové služby spojené s přenosem digitalizovaného hlasu. Z důvodu rozvoje mobilních služeb a bezdrátových sítí je VoIP komunikace i nedílnou součástí mobilních telefonů. U VoIP komunikace je vyžadována vysoká citlivost na kvalitu hovoru, který musí probíhat v reálném čase. Je však nutné zajistit, aby nedošlo např. pomocí DoS k útoku na kvalitu těchto parametrů nebo MiTM útokem k odposlechu vzájemné komunikace. Pokud by došlo k útoku, musí být odražen v max. několika sekundách, tzn. dřív, než dojde k narušení služby. U firewallů je použita detailní a hluboká analýza paketů, což je ve VoIP nepřípustné z důvodu časové náročnosti a musí se najít rozumný kompromis mezi kvalitou hovoru a jeho zabezpečením. Má bakalářská práce se zaměřuje na šifrování SIP signalizace a média paketů při vzájemné komunikaci SIP softwarových klientů na platformě Android. Platforma Android byla zvolena z důvodu, že je nejrozšířenějším operačním systémem dnes používaných mobilních telefonů a protokol SIP z důvodu, že je podporován drtivou většinou VoIP zařízení. K rozšíření signalizačního protokolu SIP došlo z důvodu, že v minulosti používaný protokol H.323 je po mnoha optimalizačních krocích příliš robustní a novější protokol IAX sice snadněji prochází přes firewally, ale nemá obecný mechanismus pro další rozšiřování funkcionalit. Protokol SIP však sám o sobě nemá žádné bezpečnostní mechanismy. Z tohoto důvodu byly navrženy způsoby, jak zabezpečit samotnou SIP signalizaci, tak přenos médií. Platforma Android podporuje instalaci vlastních aplikací, včetně SIP softwarových klientů umožňujících komunikaci na protokolu SIP. S tímto však souvisí riziko nezabezpečené VoIP komunikace, jelikož řada těchto klientů nepodporuje šifrovanou komunikaci, nebo ji nepodporuje komplexně.

Bakalářská práce má za úkol na základě praktického testování SIP softwarových klientů na platformě Android zjistit, jaké nejsilnější zabezpečení dokáží skutečně poskytnout ve vztahu k zabezpečení samotné SIP signalizace, tak i ve vztahu k samotnému šifrování přenosu médií. V následující kapitole je krátké uvedení platformy Android a jsou zde popsány protokoly pro přenos média paketů a také signalizační protokoly využívané ve VoIP. Třetí kapitola se věnuje tématu, na kterých místech je možno VoIP komunikaci zabezpečit, a jaké jsou možnosti tohoto zabezpečení. Čtvrtá kapitola je hlavním bodem této práce. Je zde seznámení se softwarem použitým při testování SIP softwarových klientů na platformě Android a výsledky testování zabezpečené komunikace mezi jednotlivými klienty. Následující kapitola doplňuje výsledky testování o srovnání jednotlivých SIP softwarových klientů, s účelem definovat nejvhodnějšího klienta pro použití v praxi. V této kapitole jsou také uvedeny návrhy vylepšení bezpečnostních algoritmů.

2 Operační systém Android a základy VoIP

V této kapitole je uveden operační systém Android a také, aby bylo možno vysvětlit jednotlivé bezpečnostní mechanismy využívané ve VoIP, je třeba uvést a porozumět jednotlivým transportním a signalizačním protokolům.

2.1 Operační systém Android

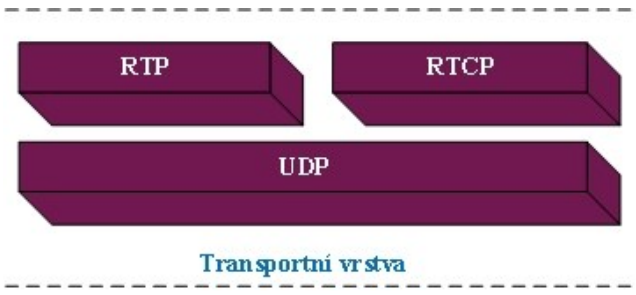
Tento operační systém je open source platforma určená především pro mobilní zařízení (chytré telefony, navigace, PDA, tablety). Je založen na Linuxovém jádru. Byl vyvinut především pro mobilní telefony a později optimalizován i pro tablety. V současné době má Android 70-ti procentní podíl na celosvětovém trhu s chytrými telefony [1, 2, 3], kdy 12% ze zbylých 30-ti procent má zastoupení konkurenční Apple v USA. 30 procent má na trhu se smartphony podíl firma Samsung (to je jedním z důvodů, proč v praktické části použijeme mobilní telefon z nabídky této firmy) [4].

Samotná platforma Android dává k dispozici nejen operační systém s uživatelským prostředím pro koncové uživatele, ale i kompletní řešení nasazení operačního systému (specifikace driverů aj.). Pro mobilní operátory a výrobce zařízení a v neposlední řadě pro vývojáře aplikací poskytuje efektivní nástroje pro jejich vývoj – Software Development Kit.

V dnešní době mobilní telefony a tablety umožňují svým vysokým výkonem a datovým připojením využívat služeb VoIP. Do systému Android byl od verze 2.3. přidán nativní SIP klient. Hrozí zde ale riziko nebezpečí ve formě nedostatečného zabezpečení provozu VoIP v bezdrátových sítích standardu 802.11.

2.2 Transportní protokoly ve VoIP

K provozu VoIP komunikace jsou používány transportní protokoly UDP (RFC 768) [5], RTP (RFC 1889, 3550) [6, 7]. Na těchto protokolech je přenášen samotný hlas či video a jiná data spojená s jejich administrací. Umístění níže popisovaných protokolů v modelu ISO/OSI je zobrazeno na obr. 2.1.



Obr. 2.1 – Vyobrazení transportních protokolů v modelu ISO/OSI.

2.2.1 RTP (Real-time Transfer protocol)

RTP protokol přenáší ve VoIP zvuk a obraz v reálném čase. Umožňuje jak přenos mezi jedním odesílatelem a jedním příjemcem (Unicast), tak i mezi jedním odesílatelem a více příjemci (Multicast). Při přenosu využívá dynamické porty.

Je protokolem transportní vrstvy, který je zadokumentovaný v IETF RFC 1889 [6] a IETF RFC 3550 [7]. Je bezestavový. Oproti UDP však přidává časovou známku a také sleduje doručení datagramů. Toto je však pro příjemce pouze informativní zpráva, která nezaručuje samotné doručení datagramů. Protokol RTP neposkytuje šifrování přenosu RTP paketů. K tomu je využit protokol SRTP nebo ZRTP. Tyto protokoly jsou rozepsány v kapitole 3.

2.2.2 RTCP (Real-time Transfer Control protocol)

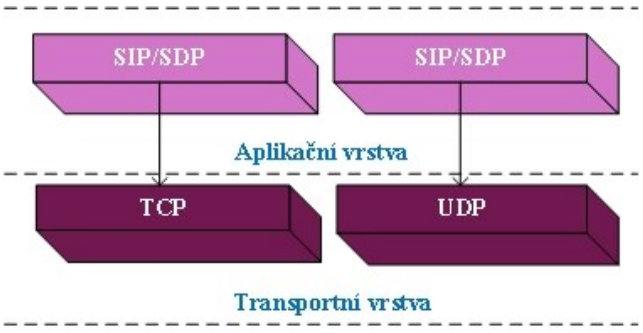
Poskytuje řídící informace pro RTP tok dat, ale sám žádná data nenese. Používá se k pravidelnému přenosu kontrolních paketů účastníkům streamované multimediální relace. Hlavní funkcí RTCP je poskytování zpětné vazby na kvalitu služeb (QoS) poskytovanou RTP. RTCP shromažďuje údaje o mediálním spojení a informace, jako například počet odeslaných bajtů, počet odeslaných paketů, počet ztracených paketů, jitter (kolísání zpoždění), zpětnou vazbu a dobu odezvy. Aplikace může tyto informace použít ke zvýšení kvality služeb například zvýšením datového toku nebo použitím jiného kodeku [7]. RTCP rovněž neposkytuje šifrování toku nebo ověření prostředků. K tomuto účelu může být použit protokol SRTCP.

2.3 Signalizační protokoly

Tyto protokoly jsou důležité pro navazování a ukončování spojení. Převážně jsou používány pro kompletní správu a řízení hovorů. Mezi tyto protokoly se řadí SIP (RFC 3261) a SDP (RFC 2327, RFC 4566). Dalšími jsou protokol H.323, který je po mnoha optimalizačních krocích příliš robustní a IAX protokol, který sice snadněji prochází přes firewally, ale nemá obecný mechanismus pro další rozšiřování funkcionalit. Majoritním signalizačním protokolem je však v současné době protokol SIP.

2.3.1 SIP (Session Initiation protocol)

Je signalizačním protokolem IP telefonie, který se používá pro zahájení, modifikaci a ukončení telefonických hovorů ve VoIP. Jeho umístění v modelu ISO/OSI je zobrazeno na obr. 2.2. SIP vyvinula IETF a jeho současná druhá verze je publikována jako RFC 3261. [8] Popisuje komunikaci potřebnou pro zahájení telefonického hovoru. Další rozšíření jsou definována v samostatných RFC.



Obr. 2.2 – Vyobrazení signalizačních protokolů v modelu ISO/OSI.

U tohoto protokolu vidíme, jak nový vzor protokolu může radikálně změnit svět VoIP. SIP se jím přehnal jako bouře. Protokol připomíná protokol HTTP, je na textové bázi a je velmi otevřený a flexibilní. Z tohoto důvodu prakticky nahradil standard H.323. SIP protokol se snaží být co nejjednodušší. Pracuje na bázi výměny žádostí a odpovědí. Pro inicializaci relací používá jak UDP port 5060, tak TCP/5060. Výměna zpráv protokolu SIP se může zasílat mezi UA i pomocí šifrovaného připojení - Secure SIP. Protokol SIP je hlavičkou paketu, jejímž prostřednictvím jsou zasílány žádosti i odpovědi a protokol SDP je tělem paketu, kde jsou uvedeny informace k zahajovanému přenosu. Samotná data jsou pak při hovoru přenášena na RTP protokolu.

SIP musí zjistit a zajistit:

- *lokalizaci účastníka* tzn. najít spoj s koncovou stanicí (User Agent),
- *stav účastníka* tzn. zda je schopen účastník navázat danou relaci (může mít např. obsazeno nebo může být přesměrován),
- *volitelné parametry účastníka* např. jaký používá typ kodeku, jaká je maximální přenosová rychlost, zda může být přenášeno i video apod.,
- *navázání spojení* je zajišťováno protokolem SDP s odkazem na datový tok nad protokolem RTP,
- *řízení právě probíhajícího spojení,* tzn. musí reagovat na změny vlastností v průběhu relace.

Metody SIP protokolu:

Metody definované v RFC 3261 [8]:

INVITE – slouží k navazování spojení, nebo u již existujícího spojení ke změně parametrů,
ACK – potvrzení o obdržení požadavku,
CANCEL – žádost k přerušení zahajované relace ještě před jejím navázáním,
REGISTER – žádost k registraci účastníka na registračním serveru,
OPTIONS – požádá o informace o možnostech volajícího, aniž by se sestavilo volání,
BYE – žádost o ukončení relace.

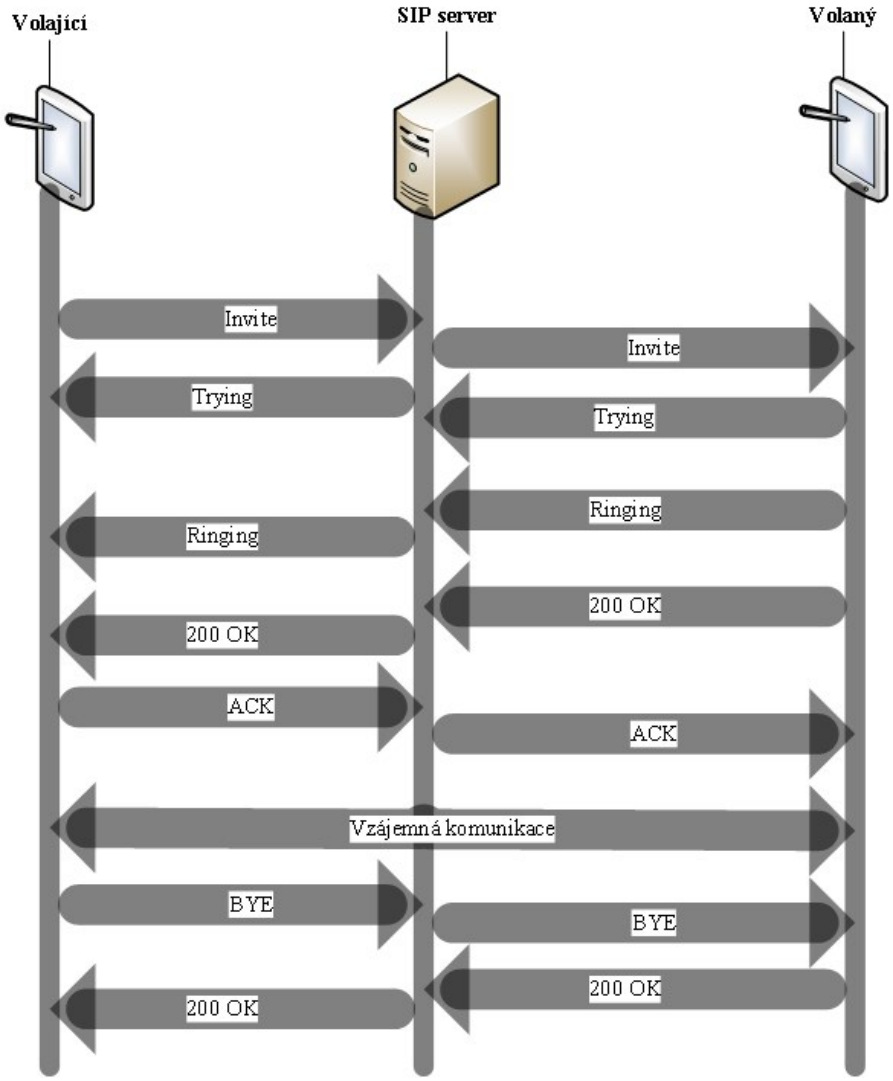
Metody definované v dalších RFC:

REFFER – požadavek jiného uživatele k řízení spojení – RFC 3515 [9],
SUBSCRIBE – požadavek pro zjištění stavu vzdáleného prvku – RFC 3265 [10],
NOTIFY – k informování koncového prvku – RFC 3265 [10],
UPDATE – aktualizace o stavu relace – RFC 3331 [11],
INFO – k přenosu informace během relace – RFC 2976 [12],
PRACK – potvrzení dočasné odpovědi – RFC 3262 [13],
MESSAGE – pro instant messaging – RFC 3428 [14].

Chybová hlášení a odpovědi protokolu mají vedle číselného označení také textovou verzi, což je uvedeno v doporučení RFC 3261 [8]:

- **1xx** – informační odpovědi, kdy byl požadavek obdržen a zpracovává se
(100 - Trying, 180 - Ringing, 182 - Queued),
- **2xx** – kladné odpovědi o tom, že požadavek byl úspěšně obdržen a zpracován bez problémů
(200 – OK, 202 - Accepted),
- **3xx** – odpovědi o přesměrování
(300 – Multiple Choices, 301 - Moved Permanently, 302 – Moved Temporarily, 305 Use Proxy),
- **4xx** – chyba na straně klienta, požadavek je chybný a nemůže být serverem zpracován
(400 – Bad Request, 403 – Forbidden, 483 – Too Many Hops),
- **5xx** – požadavek je v pořádku, ale chyba je na straně serveru
(500 – Server Internal Error, 504 – Server Time-out, 513 – Message Too Large),
- **6xx** – globální chyba
(600 – Busy Everywhere, 603 – Decline, 604 – Does Not Exist Anywhere).

SIP klienti navazují relaci přímo mezi sebou, nebo pomocí i několika SIP proxy serverů. Proxy servery mohou také plnit funkci SIP registrátora, kde se účastníci registrují. SIP pakety, jak jsme uvedli výše, nejsou při přenášení nijak zabezpečeny. Tímto se vystavujeme nebezpečí zjištění cizí osobou názvu našeho účtu a volaného a dále s tím související dané IP adresy. Také jsou sdělovány i jiné informace, např. jakého používáme SIP klienta. Komunikaci je proto nutno zabezpečit.



Obr. 2.3 Navázání komunikace na protokolu SIP

2.3.1.1 **Architektura SIP**

SIP adresa (SIP URI): Tato adresa identifikuje uživatele. Má nápadně podobný tvar, jako e-mailová adresa s tím rozdílem, že obsahuje předponu SIP (*sip:*uživatel@host). V adrese mohou být zahrnuty i nepovinné údaje, jako je port nebo parametry URI. Pokud nepovinné údaje nejsou uvedeny, předpokládá se u nich použití všeobecně známých hodnot. Např. u portu se předpokládá použití portu 5060. Při vytvoření šifrovaného připojení je místo předpony *sip* uvedena předpona *sips* [15].

Transakce: Je metoda požadavku a všech odpovědí, které na tento požadavek odpovídají. Příkladem je BYE a 200 OK [15].

Dialog: Je posloupnost SIP zpráv mezi dvěma UA, které mají vzájemnou souvislost [15].

SIP Server: Má většinou zodpovědnost za uživatele v doméně. Pracuje v módu *redirect* nebo *proxy*. V módu redirect sdělí SIP server adresu volajícího volanému, který dále navazuje spojení přímo na novou adresu. V proxy módu se spojení navazuje prostřednictvím serveru [15].

Registrar: Je registrační server, který zpracovává požadavek REGISTER a získané informace o poloze uživatele předá lokalizační službě [15].

Location Service: Tato služba poskytuje informace o aktuální IP adrese uživatele. K tomu může využít buď Radius protokol, nebo databázi s kontakty [15].

Transaction stateful proxy: Udržuje stav transakce po celou dobu od přijetí požadavku až k odeslání konečné odpovědi [15].

Call statefull proxy: Udržuje stav dialogu od prvního požadavku INVITE až do ukončovacího požadavku BYE [15].

Hlavičky SIP

To: Adresa volaného,
From: Adresa volajícího,
Via: Adresa volajícího a pokud požadavek na spojení prošel serverem, tak i jeho adresa. Stejnou cestou se bude vracet i odpověď,
Call-Id: Unikátní identifikace volání,
Contact: Aktuální skutečná adresa,
Record-Route: Obsahuje adresy serverů, které veškerou komunikaci náležící k hovoru chtějí dostávat,
Route: Postupně uvedené adresy od volajícího k volanému, včetně adres serverů, přes které je požadavek směrován,
Request-URI: Aktuální adresa volaného, která je uvedena jako první za typem metody.

2.3.2 **Protokol H.323**

Byl přijat Mezinárodní telekomunikační unií v roce 1996. V roce 2009 je vydán poslední dokument, který rozšiřuje nové doporučení a byly přidány nové funkce. Tento protokol v sobě zahrnuje spoustu dalších protokolů, čímž v porovnání se SIP protokolem je složitější pro komunikaci ve VoIP. Prostředí protokolu H.323 bylo vyvinuto tak, aby jej bylo možné použít například při pořádání videokonferencí s využitím sítí PSTN, uplatnění a splnění požadavků v multimediální komunikaci [16, 17].

2.3.3 **SDP (Session Description protocol)**

Je určený k popisu vlastností relace multimediálního přenosu dat. Nepřenáší se pomocí něj vlastní data, slouží pro vyjednání parametrů, jako je typ média (video, audio, atd.), transportní protokol (RTP/UDP/IP, H.320, TCP, atd.), typ kodeku nebo přenosová rychlost. Je popsaný v RFC 4566 [18]. Je často používán ve spojení se SIP.

3 Bezpečnost VoIP v bezdrátových sítích

Projektování, nasazení a bezpečné provozování sítě VoIP je komplexní úsilí, které vyžaduje pečlivou přípravu. Tato je však v dnešních tržních podmínkách zanedbávána a uživateli VoIP sítě někdy nezbývá nic jiného, než si zabezpečit svůj přenos ve VoIP síti sám.

Komunikace na platformě Android, pomocí protokolu SIP probíhá bezdrátovým přenosem, čímž spočívá nebezpečí VoIP komunikace především ve snadném přístupu ke komunikačnímu kanálu.

Stejně, jako je třeba zabezpečit jiné protokoly využívané v Internetu a jiných datových sítích, je třeba zabezpečit protokoly využívané ve VoIP komunikaci, v našem případě v komunikaci provozované na SIP protokolu tak, aby nemohlo dojít k žádnému z útoku uvedených v kapitole 3.1-Výčet bezpečnostních hrozeb. SIP softwarový klient by měl, pokud ho chceme považovat za bezpečného, splňovat několik bezpečnostních mechanismů. Měl by mít podporu pro přenos dat na protokolu SRTP, ideálně přenos dat na protokolu ZRTP. Další podporou SIP klienta je nutnost přenosu dat na protokolu TCP, který udržuje trvalé spojení s použitím protokolu TLS. Možnost změny portu ze standartní hodnoty 5060 na jinou hodnotu je výhodou.

Vždy pro bezpečný provoz VoIP sítě je třeba zajistit tyto procesy:

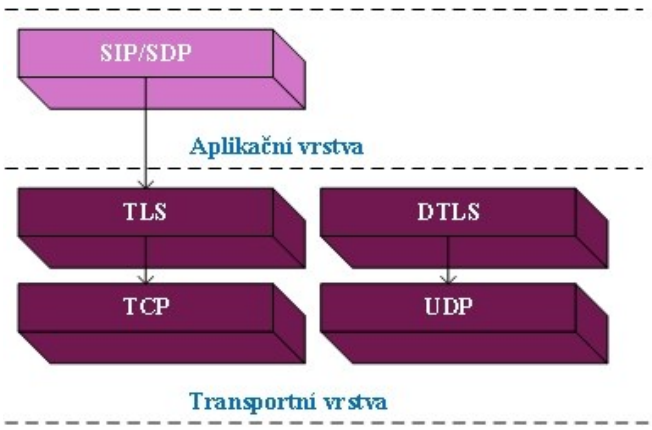
- Autentizaci [19] – ověřuje se identita komponenty, nebo uživatele za účelem ochrany proti falšování identity,
- Autorizaci [19] – je zjišťováno, zda má uživatel nebo komponenta oprávnění provádět žádanou funkci,
- Důvěru [19] – při vlastním přenosu dat musí být mezi volanými zachována vzájemná bezpečná ochrana,
- Integritu [19] – nesmí dojít během přenosu dat k jejich jakémukoliv narušení (změny nebo smazání). Data musí být po doručení stejná, jaké vyslal zdroj.

3.1 Výčet bezpečnostních hrozeb

- Monitorování s skenování VoIP sítě za účelem nalezení datového přenosu SIP klienta,
- Odmítnutí služby DoS (Denial of Service) – DoS útok na signalizační protokol SIP může být např. záplavový (flood) – neustálé zasílání SIP požadavků, krádež registrace (Registration hijacking) nebo útok za účelem ukončení spojení (Session teardown),
- Mapování čísel – sledování SIP příchozích a odchozích paketů,
- Man in the middle – zachycení, popř. pozměnění směru dat v komunikaci,
- Odebrání registrace ze SIP serveru,
- Přidání registrace SIP serveru,
- Ukončení sestaveného hovoru pomocí modifikace SIP zpráv.

3.2 Zabezpečení signalizačních protokolů

Jedním ze základních požadavků uskutečněné SIP signalizace je používání protokolů, které umožňují signalizaci zabezpečit. Umístění níže popisovaných protokolů v modelu ISO/OSI je zobrazeno na obr. 3.1.



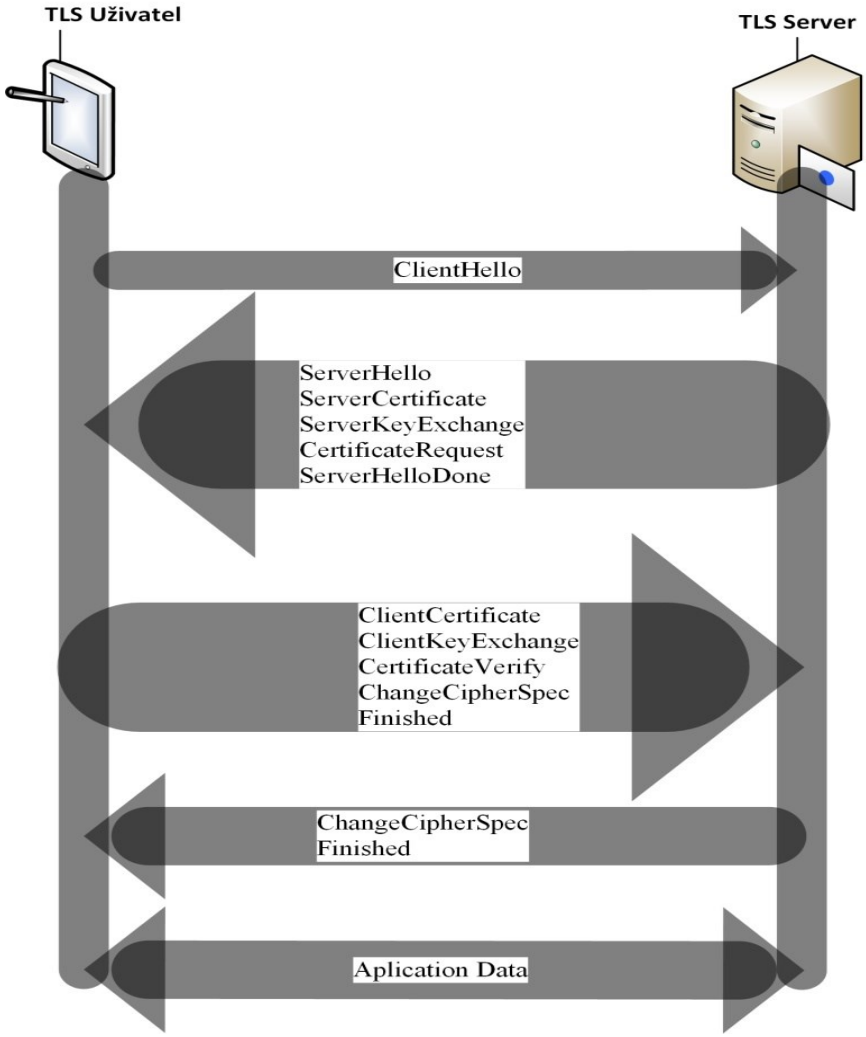
Obr. 3.1. – Vyobrazení protokolů šifrující komunikaci v modelu ISO/OSI

3.2.1 TLS (Transport Layer Security)

Protokol TLS je kryptografický protokol, který nám nabízí zabezpečenou komunikaci na Internetu, v našem případě dále pro VoIP telefonii na protokolu SIP v operačním systému Android (i v RFC 3261 je doporučeno použití TLS).

Tento protokol je účinná metoda proti odposlechu nebo zfalšování zprávy. Zajišťuje proces autentizace uživatele vůči serveru i proces vzájemné autentizace mezi uživateli, kdy však musí být zajištěna bezpečná distribuce veřejných klíčů pro jednotlivé uživatele pomocí certifikační autority.

Současná verze protokolu TLS 1.2 je definována v RFC 5246 [20]. V protokolu TLS jsou zahrnuty následující kroky. Uživatelé si vymění zprávu *ClientHello*, aby se dohodli na použitých algoritmech a výměně náhodného čísla. Poté si vymění potřebné kryptografické parametry, aby se uživatel a server dohodli na způsobu předání hlavního šifrovacího klíče (premaster key). Server následně zašle certifikát, který je zaslán ve zprávě *ServerCerificate*. Certifikát musí být založen na X.509v3, není-li výslovně sjednán jiný typ, např. TLSPGP [21].



Obr. 3.2 – Inicializace TLS komunikace.

ClientHello – počáteční domluva na parametrech spojení, oznámení nejvyšší podporované verze TLS, dále zašle náhodné číslo, seznam kryptografických a kompresních možností klienta,

ServerHello – po projití klientových seznamů server zvolí verzi protokolu, zašle náhodné číslo a vybranou šifrovací a kompresní metodu,
ServerCertificate – zpráva obsahuje certifikační řetězec,
ServerKeyExchange – zpráva obsahuje výběr algoritmu za účelem vytvoření „premaster secret", pokud předchozí zpráva *ServerCertificate* neobsahovala minimální informace, které jsou potřebné pro vytvoření premaster secret,
CertificateRequest – může být požadován klientský certifikát,
ServerHelloDone – oznámení o dokončení úvodních zpráv,

ClientCertificate – obsahuje certifikační retězec klienta,
ClientKeyExchange – nastavení „premaster secret",
CertificateVerify – ověření klientského certifikátu v případě, že má být podepsán,
ChangeCipherSpec – oznámení, že zasílána data budou šifrována,
Finished – oznámení, že dohodnuté klíče a autentizace byla úspěšně dokončena,

Aplication Data – již zabezpečená (šifrovaná) přenášená data na bázi TCP spojení [21].

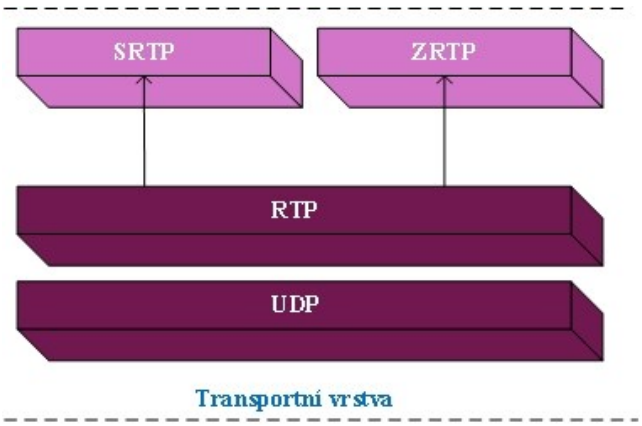
Grafické zobrazení TLS komunikace je zobrazeno na obr. 3.2. V našem případě při testování SIP softwarových klientů budeme využívat protokol UDP, který se enkapsuluje do protokolu TCP a následně do protokolu TLS. Tak probíhá komunikace na SIP protokolu za použití protokolu TLS. Protokol TLS tedy pracuje nad protokolem TCP, který zaručuje doručení dat ve správném a úplném pořadí.

3.2.2 DTLS (Datagram Transport Layer Security)

Je protokol, který pracuje nad protokolem UDP. Jeho využití je u aplikací, kde nízká ztrátovost paketů může být tolerována, tzn. že nachází uplatnění ve VoIP komunikaci. Protokol DTLS je využíván pro šifrování komunikace v reálném čase na protokolu WebRTC. Protokol DTLS je definován v RFC 4347 [22].

3.3 Zabezpečení transportních protokolů

Dalším základním požadavkem je zabezpečení přenosu samotných RTP paketů, které nesou samotná data. Bez tohoto zabezpečení by data byla po odchycení RTP paketů jednoduše reprodukovatelná. Umístění níže popisovaných protokolů v modelu ISO/OSI je zobrazeno na obr. 3.3.



Obr. 3.3 – Vyobrazení transportních protokolů SRTP a ZRTP v modelu ISO/OSI.

3.3.1 SRTP (Secure Real-time Transfer protocol)

Je protokolem transportní vrstvy, který je zadokumentovaný v IETF RFC 3711 [23]. Je to bezpečná varianta RTP protokolu. Je zde použita symetrická šifra, většinou AES (Advanced Encryption Standard). Dále integritu a autentizaci zprávy zajišťuje mechanismus HMAC-SHA1 (Keyed-Hash Message Authentication Code SHA1). Tento protokol na základě master key zajistí session keys každé relaci, čímž docílíme, že tyto session keys budou pro zajištění integrity a autentizace pro každou jednotlivou relaci jiné. Master key jsou většinou vzájemně předávány metodou MIKEY (Multimedia Internet KEY). Potřebná data jsou předávána pomocí SIP signalizace u SDP (Session Description protocol) zprávy.

Protokol SRTP tedy sám nedokáže zabezpečit výměnu klíčů, ale používá např. protokol MIKEY, který je zapouzdřený v protokolu SDP. Celý obsah je však nešifrovaný vyjma dohodnutí bezpečnostních šifrovacích a autentifikačních algoritmů. Přenáší tedy přímo i master key, proto je důležité zabezpečit SIP signalizaci např. pomocí protokolu TLS. Bez protokolu TLS jsou odposlechnutelné použité klíče a potom i celý hovor.

3.3.2 ZRTP (Zimmermann RTP)

ZRTP je protokolem transportní vrstvy, který je popsán v IETF RFC 6189 [24]. Protokol ZRTP rozšiřuje protokol SRTP o zabezpečenou výměnu klíčů, která je založena na metodě Diffie-Hellman (Účastnící VoIP komunikace si díky tomuto algoritmu vypočtou své vnitřní klíče, které se na přenosové cestě nikdy neobjeví. Veřejné a vnitřní klíče tedy vždy vznikají na začátku hovoru a zanikají s ukončením hovoru.) [25]. Tento protokol také obsahuje systém SAS (Short Authentication Strings) ke zjištění případného Man in the middle útoku.

ZRTP je určen pouze k šifrování RTP paketů, tj. audio, nebo i video, jenž jsou přenášeny mezi dvěmi UA. ZRTP lze také doplnit o Preshared mode, kdy jsou veřejné klíče přeneseny mezi UA u prvního spojení a tyto se nevymazávají, ale část z nich se cachuje. Díky tomuto se pak jen vypočtou šifry u případných dalších hovorů mezi stejnými UA. Tímto preshared mode se odlehčí výpočet procesoru UA [26]. Protokol ZRTP se hlavně využívá k ustanovení klíčů pro protokol SRTP.

3.4 Zabezpečení Wi-fi přenosu

Po seznámení se s jednotlivými protokoly a dříve, než se zaměříme na jejich podporu u testovaných SIP softwarových klientů, jenž zabezpečují VoIP komunikaci proti bezpečnostním hrozbám, zde krátce uvedeme bezpečnostní rizika u datového přenosu na síti Wi-fi, jelikož připojení k Internetu je na zařízeních s OS Android provozujících SIP softwarového klienta výlučně pomocí Wi-fi.

Android má vestavěného VPN klienta, který podporuje PPTP (na konci července 2012 byl prolomen šifrovací protokol MS-CHAPv2, proto nelze použití PPTP VPN považovat za bezpečné), L2TP a IPSec s pre-shared key nebo zabezpečení pomocí certifikátu.

Mimo výše uvedené je zapotřebí Wi-fi síť zabezpečit autentizačními algoritmy WPA, nebo WPA2. WPA2 používá novější šifru AES. Toto téma není však v této bakalářské práci dále rozvedeno, jelikož není jejím předmětem.

3.5 Požadavky na SIP softwarového klienta z pohledu bezpečnosti

Na základě výše uvedených bezpečnostních metod v IP telefonii je tedy vhodné, aby SIP softwarový klient podporoval přenos zabezpečených RTP paketů protokolem SRTP, ideálně protokolem ZRTP. Dále, aby podporoval zabezpečení SIP signalizace pomocí protokolu TLS. Tento protokol v základním nastavení využívá port 5061. Nezabezpečený přenos dat na protokolu UDP nebo TCP v základním nastavení využívá port 5060. Změna portu, kde datový přenos probíhá je také výhodou. Touto změnou můžeme před případným útočníkem skrýt, že vůbec nějaká komunikace probíhá.

Bez zabezpečení SIP signalizace protokolem TLS je po odchycení VoIP komunikace zjistitelná IP adresa volajícího, volaného a telefonní ústředny, název a verze softwaru (SIP klienta), port na kterém jsou domlouvány podmínky spojení, uživatelské jméno volajícího a volaného, označení hardwarového zařízení (typ telefonu), na kterém je SIP klient nainstalován, transportní protokol na kterém VoIP signalizace probíhá, typ použitého audio-kodeku, jaký algoritmus je použit u hashovací funkce. Tyto informace jsou už dostačující k tomu, aby případný útočník, který má zájem na odchycení VoIP komunikace nebo na podstrčení identity se dále snažil svůj útok realizovat.

Pokud nejsou RTP pakety šifrovány pomocí protokolů SRTP, nebo ZRTP, tak např. síťový analyzátor Wireshark z nich po odchycení vytvoří audio soubor se zachycenou VoIP komunikací.

Proto je tedy důležité VoIP komunikaci zabezpečit, ať už samotnou signalizaci nebo přenos RTP paketů.

4 Testování

Po všeobecném seznámení se s protokoly zabezpečujícími VoIP komunikaci budou tyto znalosti využity v praktickém testování jednotlivých SIP softwarových klientů na platformě Android, což je hlavní částí této bakalářské práce.

4.1 Použitý software pro testování

Ke zjištění úrovně zabezpečení a případných důvodů nekompatibility jednotlivých SIP klientů byl využit níže uvedený software.

4.1.1 Asterisk

K vzájemnému testování jednotlivých SIP softwarových klientů byla využita open source telefonní ústředna Asterisk, která je plně kompatibilní s protokolem SIP. Instalace Asterisku byla provedena pomocí kompilace zdrojových kódů, kdy byla nainstalována v současné době nejvyšší verze 11.2.1 na unixovém operačním systému Ubuntu LTS verzi 12.04. Instalace Asterisku byla provedena za pomocí níže uvedených příkazů.

Stažení SRTP knihovny nutné pro provoz protokolu SRTP:

```
wget http://sourceforge.net/projects/srtp/files/srtp/1.4.4/srtp-
1.4.4.tgz
```

instalace kernel hlaviček:

```
apt-get install linux-headers- "uname -r"
```

další balíčky potřebné pro kompilaci Asterisku:

```
apt-get install libssl-dev ncurses-dev
```

stáhnutí zdrojových kódů z repozitářů Asterisku:

```
wget http://downloads.asterisk.org/pub/telephony/asterisk/releases
/asterisk-11.2.1.tar.gz
wget http://downloads.asterisk.org/pub/telephony/libpri/releases
/libpri-1.4.14.tar.gz
wget http://downloads.asterisk.org/pub/telephony/asterisk/releases
/asterisk-addons-1.6.2.4.tar.gz
```

dekomprimace stažených souborů:

```
tar -xvzf asterisk-11.2.1.tar.gz && tar -xvzf lippri-1.4.14.tar.gz
&& tar -xvzf asterisk-addons-1.6.2.4.tar.gz
```

dále za použití níže uvedených příkazů dokončíme instalaci Asterisku:

```
make all
make install
make config
./configure
make menuselect
make config
```

Po instalaci Asterisku pomocí *ast_tls_cert* skriptu umístěném v *contrib/scripts* ve zdrojovém adresáři Asterisku byla vytvořena self-signed certifikační autorita a Asterisk certifikát [27].

```
./ast_tls_cert -C 192.168.1.105 -O "man089" -d /etc/asterisk/keys
```

"`-C`" slouží k definování našeho počítače (192.168.1.105 – IP adresa Asterisku),
"`-O`" definice názvu,
"`-d`" výstupní adresář klíčů.

Po vytvoření certifikační autority a Asterisk certifikátu byly vygenerovány dva klientské certifikáty pro SIP softwarové klienty [27].

```
./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k
/etc/asterisk/keys/ca.key -C SamsungNexus.192.168.1.105 -O "man089"
-d /etc/asterisk/keys -o SamsungNexus
```

```
./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k
/etc/asterisk/keys/ca.key -C SonyST15i.192.168.1.105 -O "man089" -d
/etc/asterisk/keys -o SonyST15i
```

"`-m client`" říká skriptu, že chceme vytvořit klientský certifikát,
"`-c /etc/asterisk/keys/ca.crt`" specifikuje certifikační autoritu, kterou používáme,
"`-k /etc/asterisk/keys/ca.key`" poskytuje klíč k výše definovné CA,
"`-C`" nastavení IP adresy nebo hostname SIP telefonu,
"`-O`" definice názvu,
"`-D`" výstupní adresář pro klíče,
"`-o`" název výstupního klíče [27].

V adresáři */etc/asterisk/keys* nyní máme tyto klíče: *asterisk.crt, asterisk.csr, asterisk.key, asterisk.pem, SamsungNexus.crt, SamsungNexus.csr, SamsungNexus.key, SamsungNexus.pem, SonyST15i.crt, SonyST15i.csr, SonyST15i.key, SonyST15i.pem, ca.cfg, ca.crt, ca.key, tmp.cfg.*

Dále bylo pro naše potřeby testování v konfiguračním souboru *sip.conf* nastaveno:

`tlsenable=yes` – povolujeme použití TLS,
`tlsbindaddr=0.0.0.0` – jsme vázáni na naši lokální IPv4 adresu,
`tlscertfile=/etc/asterisk/keys/asterisk.pem` –cesta k vytvořenému certifikátu TLS,
`tlscafile=/etc/asterisk/keys/ca.crt` – cesta k vytvořené certifikační autoritě,
`tlscipher=ALL` – výběr TLS šifer byl nastaven na ALL,

`tlsclientmethod=tlsv1` – pro klienta byla vybrána šifrovací metoda TLSv1, podle RFC by dostupní klienti měli tuto normu podporovat [27].

Níže je uvedeno nastavení účtu při testování SIP softwarového klienta, kdy bude komunikace probíhat současně na protokolu TLS pro signalizaci a SRTP pro přenos médií, což bylo provedeno v *sip.conf*.

```
[2001];SamsungNexus
type=peer
secret=1234
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=g722
allow=ulaw
transport=tls
srtpcapable=yes
```

4.1.2 Wireshark

Je síťový analyzátor, který umožňuje zachytávat a analyzovat síťovou komunikaci [28]. Bude následně využit v části při testování SIP softwarových klientů ve VoIP komunikaci za účelem zjištění, zda komunikace probíhá zabezpečeně a také ke zjištění důvodů, proč nejsou někteří klienti mezi sebou kompatibilní.

4.2 Použitý hardware pro testování

K testování byl pro oblíbenost u uživatelů použit smartphone Samsung Galaxy [29] s přívlastkem Nexus pro otevřenost operačního systému Android od společnosti Google. Na tomto smartphone s označení i9250 je nainstalován operační systém Android 4.1.1 [30]. Druhým smartphonem byl SonyEricsson ST15i z řady Xperia mini s operačním systém Android 4.0.4 [31]. Tento byl vybrán z důvodu oblíbenosti u českých uživatelů, jelikož má výborný poměr cena/výkon.

Žádný z výše uvedených smartphonů neměl problém s nainstalováním jakéhokoliv SIP softwarového klienta.

4.2.1 Výběr SIP softwarových klientů

Prvním kritériem při výběru SIP softwarových klientů byla jejich nezávislost na předdefinovaných VoIP providerech, jelikož úkolem této bakalářské práce je otestovat SIP softwarové klienty a nikoliv kvalitu zabezpečení VoIP komunikace na protokolu SIP jednotlivých poskytovatelů této služby. Z více než 160-ti SIP softwarových klientů, kteří byli vyhledání pomocí internetových vyhledávačů a na Google Play Store, bylo pouze 31 nezávislích na VoIP providerech. Někteří SIP klienti měli však na výběr z více než 80-ti poskytovatelů VoIP telefonie. Toto testování bylo prováděno tak, že každý SIP klient byl nainstalován na smartphone s operačním systémem

Android, byla otestována jeho nezávislost na předdefinovaných providerech v uživatelském rozhraní a následně odinstalována, jelikož někteří SIP softwaroví klienti měli snahu o integrování se do systému Android a následně ovlivňovat jiné SIP softwarové klienty bez možnosti souhlasu či zamítnutím této volby uživatelem.

Druhým kritériem byla podpora protokolu SRTP. Z 31 klientů (tabulka uvedena v příloze I), kteří prošli prvním kritériem jich pouze 12 podporuje protokol SRTP. Klient is-Phone deklaroval, že podporuje tento protokol. Při prvním testování spojení, kdy klienti měli v *sip.conf* Asterisku nastaveno `srtpcapable=yes`, tzn. nutná podmínka pro navázání komunikace je, že bude probíhat na protokolu SRTP, bylo Asteriskem oznámeno varování uvedené na obr. 4.1.

```
WARNING[2754][C-00000006]: chan_sip.c:10433 process_sdp: We are requesting SRTP for audio, but they responded without it!
```

Obr. 4.1 – Varování Asterisku o snaze SIP klienta navázat spojení bez protokolu SRTP.

Tímto Asterisk dával na vědomí, že SIP klient nepodporuje protokol SRTP a komunikace nebude zahájena bez jeho podpory SIP klientem a Asterisk spojení ukončil. Neschopnost tohoto klienta navázat spojení na protokolu SRTP při testování je dále uvedena v tabulkách 4.2, 4.4.

Dále bylo prováděno zjištění důvodů níže uvedeného varování ve Wiresharku, kde po odchycení paketu bylo zjištěno, že se jedná o chybové hlášení protokolu SIP s číslem 488 – Not accetable here, čímž bylo SIP klientovi sděleno, že jeho žádosti o spojení bez protokolu SRTP nebylo vyhověno. Klient se tedy nedohodnul pomocí protokolu SDP na podmínkách spojení.

```
⊟ Session Initiation Protocol (488)
  ⊟ Status-Line: SIP/2.0 488 Not acceptable here
      Status-Code: 488
```

Obr. 4.2 – Výpis chybového hlášení zachyceného Wiresharkem

U testování podpory protokolu SRTP u SIP softwarových klientů bylo také zjišťováno, zda podporují protokol ZRTP pro zabezpečení přenosu médií. Tímto se dostavil výsledek, že z 31 testovaných klientů podporují protokol ZRTP pouze 4 SIP klienti.

Třetím kritériem byla podpora protokolu TLS, aby byla zabezpečena SIP signalizace.Tímto testováním bylo zjištěno, že 9 z 31 SIP klientů podporuje komunikaci na protokolu TLS.

Posledním kritériem byla možnost vložení vlastních certifikátů vytvořených za účelem bezpečné komunikace na protokolu TLS z pohledu zaručení autentizace strany klienta a serveru. Tímto bylo zjištěno, že pouze 1 SIP softwarový klient, kterým je CSipSimple, tuto možnost podporuje. V tabulce č. 4.1 je uveden seznam testovaných SIP softwarových klientů.

Název SIP softwarového klienta	Vlastní certifikáty	TLS	SRTP	ZRTP
CSipSimple	Ano	Ano	Ano	Ano
AcrobitsSoftphone	Ne	Ano	Ano	Ano
Groundwire	Ne	Ano	Ano	Ano
Bria	Ne	Ano	Ano	Ne
COCOS VoIP	Ne	Ano	Ano	Ne
iPhytter	Ne	Ano	Ano	Ne
Media5-fone	Ne	Ano	Ano	Ne
Voip by antisip	Ne	Ano	Ano	Ne
is-Phone	Ne	Ano	Ano	Ne
MizuDroid	Ne	Ne	Ano	Ano
Gurucom	Ne	Ne	Ano	Ne
rDialer	Ne	Ne	Ano	Ne
ABTOVoIP	Ne	Ne	Ne	Ne
AdoreSoftPhone	Ne	Ne	Ne	Ne
AGEphone	Ne	Ne	Ne	Ne
GenieDialer	Ne	Ne	Ne	Ne
MobiSIP	Ne	Ne	Ne	Ne
Nativní SIP klient	Ne	Ne	Ne	Ne
Paxos FS	Ne	Ne	Ne	Ne
Phonalisa	Ne	Ne	Ne	Ne
SessionTalk	Ne	Ne	Ne	Ne
Sipdroid	Ne	Ne	Ne	Ne
SipFoize	Ne	Ne	Ne	Ne
SipTarPhone	Ne	Ne	Ne	Ne
SipTurk	Ne	Ne	Ne	Ne
TalkYouLite	Ne	Ne	Ne	Ne
TiviPhone	Ne	Ne	Ne	Ne
Voicemailtel	Ne	Ne	Ne	Ne
VYPER	Ne	Ne	Ne	Ne
YouMagic	Ne	Ne	Ne	Ne
Zoiper	Ne	Ne	Ne	Ne

Tabulka 4.1 – Seznam testovaných SIP softwarových klientů.

4.3 Vlastní testování

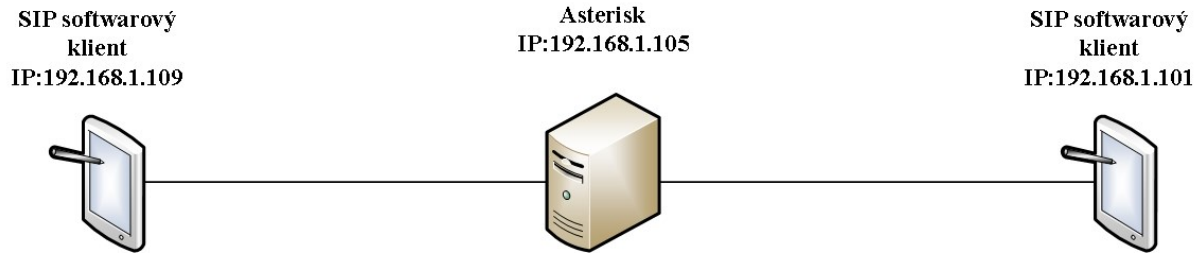
V této kapitole budou postupně uvedeny výsledky testování mezi jednotlivými SIP softwarovými klienty, kdy u těchto bude postupně nastavováno: TLS - ano a SRTP - ne , TLS - ne a SRTP - ano, TLS - ano a SRTP - ano. Každý z těchto případů byl ověřen v kombinacích: Android SIP klient - Asterisk - PC klient (Linphone a PhonerLite), Android SIP klient - Asterisk - Android SIP klient a nakonec bylo testováno spojení mezi klienty bez Asterisku navzájem, kdy byla volána IP adresa klienta.

Do testování byli zahrnuti SIP softwaroví klienti, kteří jsou uvedení v tabulce č.1 podbarveni. Jedná se o CSipSimple, AcrobitsSoftphone, Groundwire, Bria, COCOS VoIP, iPhytter, Media5-fone, Voip by antisip, is-Phone, MizuDroid.

Testování probíhalo tak, že na počítači s naistalovaným Asteriskem byl spuštěn Wireshark pomocí kterého byly odchytávány pakety SIP komunikace a následně analyzovány.

4.3.1 Testování zabezpečené komunikace SIP klient – Asterisk – SIP klient

Při tomto testování bude uvedeno, jak úspěšné je navázání komunikace SIP softwarových klientů nainstalovaných na operačním systému Android s šifrováním SIP signalizace pomocí TLS, aktivním šifrováním RTP paketů pouze pomocí protokolu SRTP, šifrováním SIP signalizace pomocí protokolu TLS spolu s aktivním šifrováním RTP paketů na protokolu SRTP. Schéma zapojení je uvedeno na obr. 4.3.



Obr. 4.3 Schéma zapojení SIP klient – Asterisk – SIP klient.

4.3.1.1 Testování SIP softwarových klientů s šifrováním SIP signalizace pomocí TLS mezi SIP softwarovými klienty prostřednictvím tel. ústředny Asterisk

Do tohoto testování byli zahrnuti všichni SIP softwaroví klienti na operačním systému Android, kteří byli vyhledáni a podporují komunikaci na protokolu TLS. Jedná se o SIP softwarové klienty: CSipSimple, Groundwire, AcrobitsSoftphone, COCOS VoIP, Media5-fone, Voip by antisip, Bria, iPhytter, is-Phone.

V následující tabulce č. 4.2 jsou uvedeny výsledky testování, kde je uvedeno, kteří SIP klienti na protokolu TLS úspěšně dohodli podmínky spojení a následně zrealizovali datový přenos.

Úspěšnost navázání komunikace SIP klient – Asterisk – SIP klient na protokolu TLS									
Volající	Volaný								
	CSip Simple	**COCOS VoIP**	**Ground-wire**	**Acrobits Softphone**	**Media5-fone**	**Voip by antisip**	**Bria**	**iPhytter**	**is-Phone**
CSipSimple	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
COCOS VoIP	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Groundwire	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Acrobits Softphone	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Media5-fone	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Voip by antisip	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Bria	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
iPhytter	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
is-Phone	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano

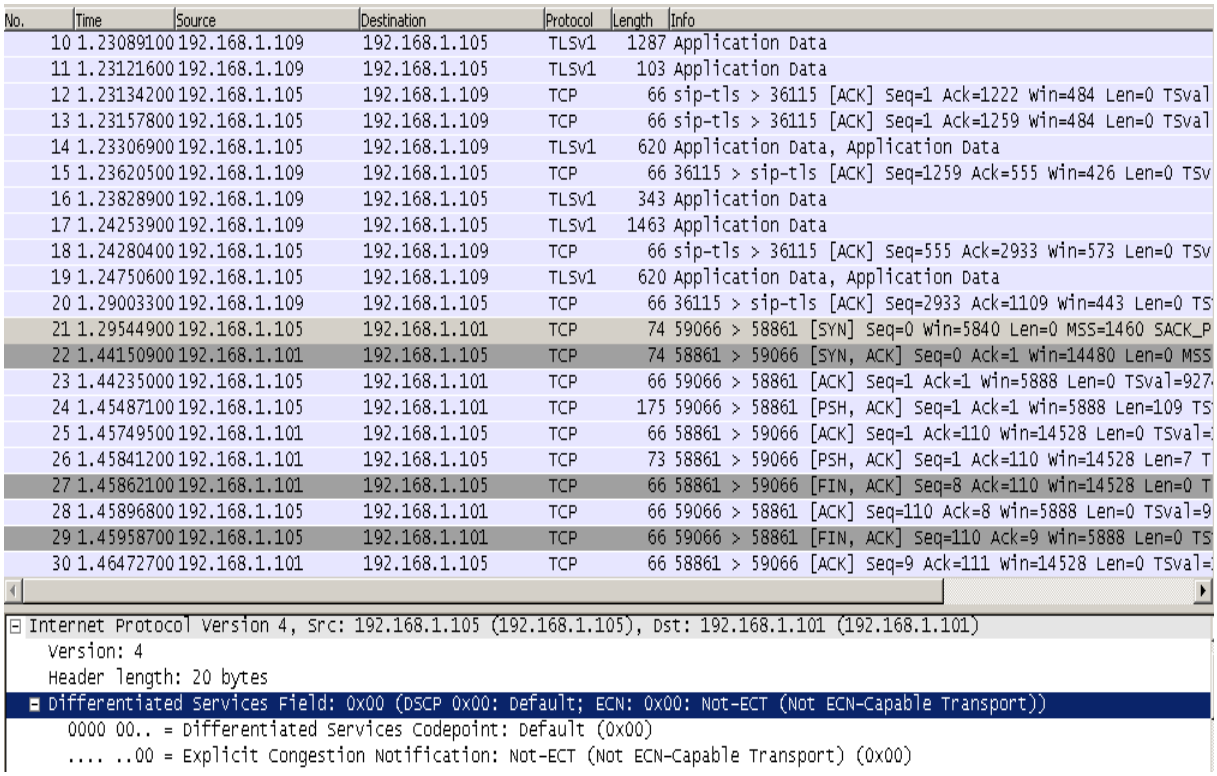
Tabulka 4.2 – Výsledky testování SIP softwarových klientů na protokolu TLS při navazování spojení mezi sebou navzájem prostřednictvím tel. ústředny Asterisk.

Při snaze o vyjednání spojení SIP softwarových klientů COCOS VoIP, Groundwire, AcrobitsSoftphone, Media5-fone, Voip by antisip, Bria, iPhytter, is-Phone se SIP klientem CSipSimple nebo Bria telefonní ústředna Asterisk oznamovala následující varování uvedené na obr. 4.4.

```
SSL certificate ok
  == Problem setting up ssl connection: error:14094410:lib(20):SSL3_READ_BYTES:sslv3 alert handshake failure
                WARNING[4517]: tcptls.c:261 handle_tcptls_connection: FILE * open failed!
```

Obr. 4.4 Varování Asterisku při snaze o navázání vzájemné komunikace SIP softwarových klientů na protokolu TLS.

Analýzou ve Wiresharku bylo zjištěno, že komunikace SIP softwarových klientů s Asteriskem probíhá v pořádku a na zabezpečeném spojení za účelem vyjednání podmínek spojení. Tyto ale vyjednány nebyly. CSipSimple na IP adrese 192.168.1.101 na řádku 22 obr. 4.5 oznamuje Asterisku zprávu Not-ECN-Capable Transport, čímž oznamuje vyjímku, že není schopen navázat přenos.



No.	Time	Source	Destination	Protocol	Length	Info
10	1.23089100	192.168.1.109	192.168.1.105	TLSv1	1287	Application Data
11	1.23121600	192.168.1.109	192.168.1.105	TLSv1	103	Application Data
12	1.23134200	192.168.1.105	192.168.1.109	TCP	66	sip-tls > 36115 [ACK] Seq=1 Ack=1222 Win=484 Len=0 TSval
13	1.23157800	192.168.1.105	192.168.1.109	TCP	66	sip-tls > 36115 [ACK] Seq=1 Ack=1259 Win=484 Len=0 TSval
14	1.23306900	192.168.1.105	192.168.1.109	TLSv1	620	Application Data, Application Data
15	1.23620500	192.168.1.109	192.168.1.105	TCP	66	36115 > sip-tls [ACK] Seq=1259 Ack=555 Win=426 Len=0 TSv
16	1.23828900	192.168.1.109	192.168.1.105	TLSv1	343	Application Data
17	1.24253900	192.168.1.109	192.168.1.105	TLSv1	1463	Application Data
18	1.24280400	192.168.1.105	192.168.1.109	TCP	66	sip-tls > 36115 [ACK] Seq=555 Ack=2933 Win=573 Len=0 TSv
19	1.24750600	192.168.1.105	192.168.1.109	TLSv1	620	Application Data, Application Data
20	1.29003300	192.168.1.109	192.168.1.105	TCP	66	36115 > sip-tls [ACK] Seq=2933 Ack=1109 Win=443 Len=0 TS
21	1.29544900	192.168.1.105	192.168.1.101	TCP	74	59066 > 58861 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_P
22	1.44150900	192.168.1.101	192.168.1.105	TCP	74	58861 > 59066 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS
23	1.44235000	192.168.1.105	192.168.1.101	TCP	66	59066 > 58861 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=927
24	1.45487100	192.168.1.105	192.168.1.101	TCP	175	59066 > 58861 [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=109 TS
25	1.45749500	192.168.1.101	192.168.1.105	TCP	66	58861 > 59066 [ACK] Seq=1 Ack=110 Win=14528 Len=0 TSval=
26	1.45841200	192.168.1.101	192.168.1.105	TCP	73	58861 > 59066 [PSH, ACK] Seq=1 Ack=110 Win=14528 Len=7 T
27	1.45862100	192.168.1.101	192.168.1.105	TCP	66	58861 > 59066 [FIN, ACK] Seq=8 Ack=110 Win=14528 Len=0 T
28	1.45896800	192.168.1.105	192.168.1.101	TCP	66	59066 > 58861 [ACK] Seq=110 Ack=8 Win=5888 Len=0 TSval=9
29	1.45958700	192.168.1.105	192.168.1.101	TCP	66	59066 > 58861 [FIN, ACK] Seq=110 Ack=9 Win=5888 Len=0 TS
30	1.46472700	192.168.1.101	192.168.1.105	TCP	66	58861 > 59066 [ACK] Seq=9 Ack=111 Win=14528 Len=0 TSval=

Obr. 4.5 – Zachycení komunikace mezi SIP softwarovými klienty a CSipSimple.

Toto varování může být tedy zapříčiněno snahou komunikovat pomocí protokolu SSLv3 a ne pomocí protokolu TLS. Varování vzhledem k množství SIP klientů, kteří nedokáží s CSipSimple komunikovat nebude v samotné telefonní ústředně Asterisk, ale v SIP softwarovém klientu CSipSimple. Stejné varování Asterisku bylo zobrazeno i v případě, že CSipSimple používal klientské certifikáty vygenerované pro Asterisk.

Stejné varovné hlášení jako u CSipSimple má další softwarový SIP klient Bria se stejným výsledkem po odchycení komunikace ve Wiresharku. Tyto varování mohou být také zapříčiněny z důvodu nedodržování RFC doporučení u protokolu TLS.

4.3.1.2 Testování SIP softwarových klientů s aktivním šifrováním RTP paketů pomocí SRTP mezi SIP softwarovými klienty prostřednictvím tel. ústředny Asterisk

Do testování byli zařazeni klienti, kteří dokáží navázat spojení na protokolu SRTP, ale mohou komunikovat i na protokolu TLS. Jedná se o SIP softwarové klienty: CSipSimple, Groundwire, AcrobitsSoftphone, COCOS VoIP, Media5-fone, Voip by antisip, Bria, iPhytter, is-Phone.

V následující tabulce č. 4.3 jsou uvedeny výsledky testování, kde je uvedeno, kteří SIP klienti na protokolu SRTP úspěšně pomocí protokolu SDP dohodli podmínky spojení a následně zrealizovali datový přenos.

Úspěšnost navázání komunikace SIP klient – Asterisk – SIP klient na protokolu SRTP									
Volající	Volaný								
	CSip Simple	**COCOS VoIP**	**Ground-wire**	**Acrobits Softphone**	**Media5-fone**	**Voip by antisip**	**Bria**	**iPhytter**	**is-Phone**
CSipSimple	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
COCOS VoIP	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
Groundwire	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
Acrobits Softphone	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
Media5-fone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Voip by antisip	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
Bria	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
iPhytter	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
is-Phone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**

Tabulka 4.3 – Výsledky testování SIP softwarových klientů na protokolu SRTP při navazování spojení mezi sebou navzájem prostřednictvím tel. ústředny Asterisk.

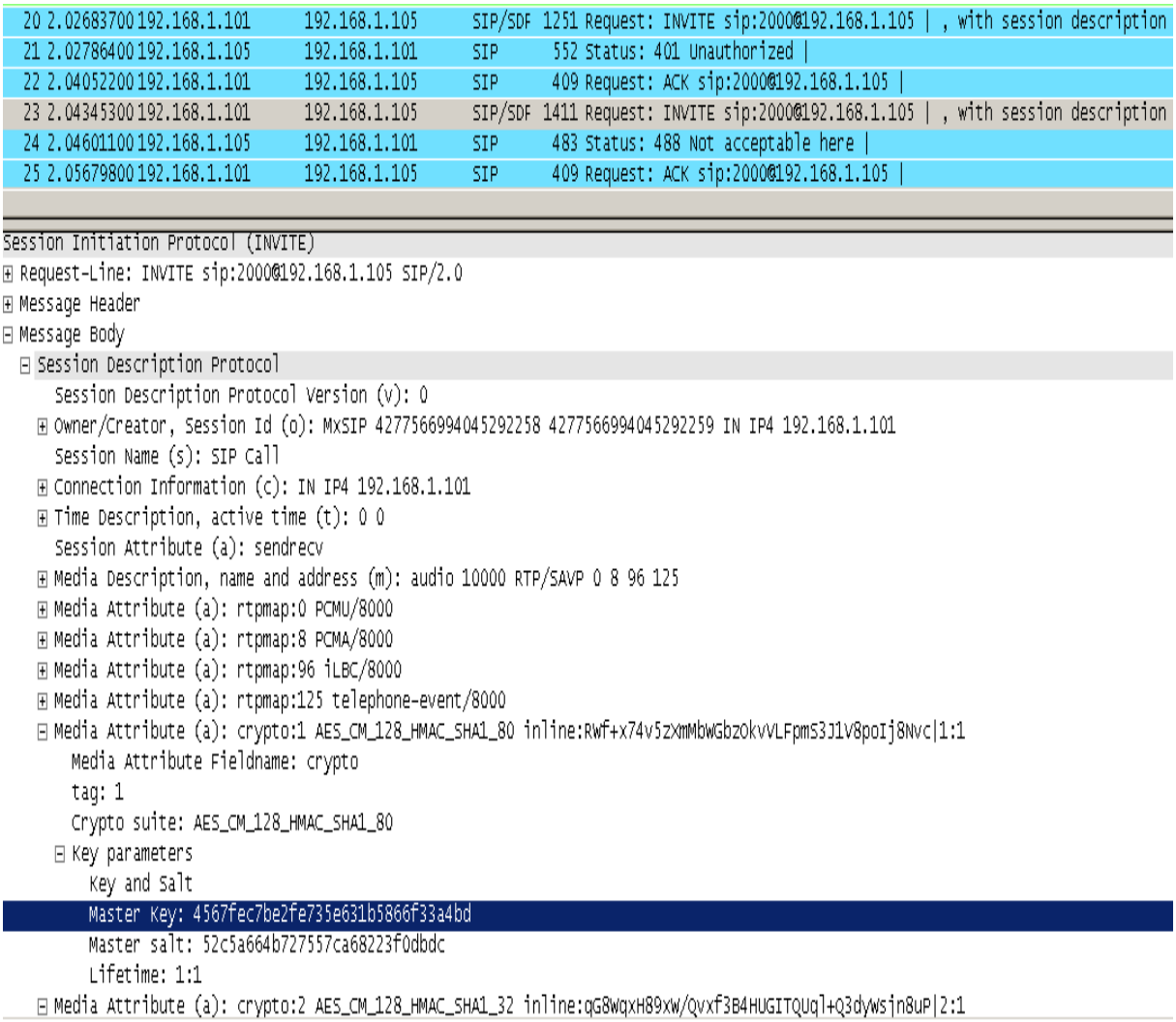
Media5-fone nedokáže navázat spojení z důvodu varování Asteriskem, které je uvedeno na obr. 4.6. Toto varování je rozšířeno o oznámení, která jsou také na obr. 4.6. zachycena.

```
NOTICE[9501][C-00000007]: sip/sdp_crypto.c:250 sdp_crypto_process: Crypto life time unsupported: crypto:1 A
ES_CM_128_HMAC_SHA1_80 inline:GOVzdS115mTL8zmA9FcKACABcdaiIZtZh8yPWHSl|1:1
NOTICE[9501][C-00000007]: sip/sdp_crypto.c:260 sdp_crypto_process: SRTP crypto offer not acceptable
NOTICE[9501][C-00000007]: sip/sdp_crypto.c:250 sdp_crypto_process: Crypto life time unsupported: crypto:2 A
ES_CM_128_HMAC_SHA1_32 inline:EpEJBF2XtoPLbYycUkv7Jer8Ed4dR843eKVE25PX|2:1
NOTICE[9501][C-00000007]: sip/sdp_crypto.c:260 sdp_crypto_process: SRTP crypto offer not acceptable
WARNING[9501][C-00000007]: chan_sip.c:10427 process_sdp: Can't provide secure audio requested in SDP offer
```

Obr. 4.6 – Oznámení spolu s varováním Asterisku při snaze navázat spojení klientem Media5-fone s ostatními klienty.

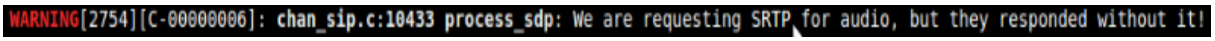
Tímto Asterisk spolu s varováním oznamuje, že nemůže s klientem Media5-fone vyměnit master key podle kterého se následně generují session keys, k čemuž byl použit protokol SDP. Protokol SDP neposkytuje žádnou ochranu zabezpečení a v tomto testování nebyl použit protokol TLS, proto můžeme na varování spolu s oznámením nahlédnout podrobněji, oproti následujícímu testování při kterém byl použit k navázání vzájemné komunikace i protokol TLS.

Zachycená komunikace síťovým analyzátorem Wireshark je uvedena na obr. 4.7. Zde lze vidět, že u předávání Master key šifrovací metodou AES_CM_128_HMAC_SHA1_80, která je navržena k výměně klíčů v RFC 4568 na protokolu SDP, je porušeno pravidlo režimu Counter Mode šifrovací metody AES. Opět tedy nedochází k vyjednání podmínek spojení a je oznámena chyba č. 488 – Not accetable here.

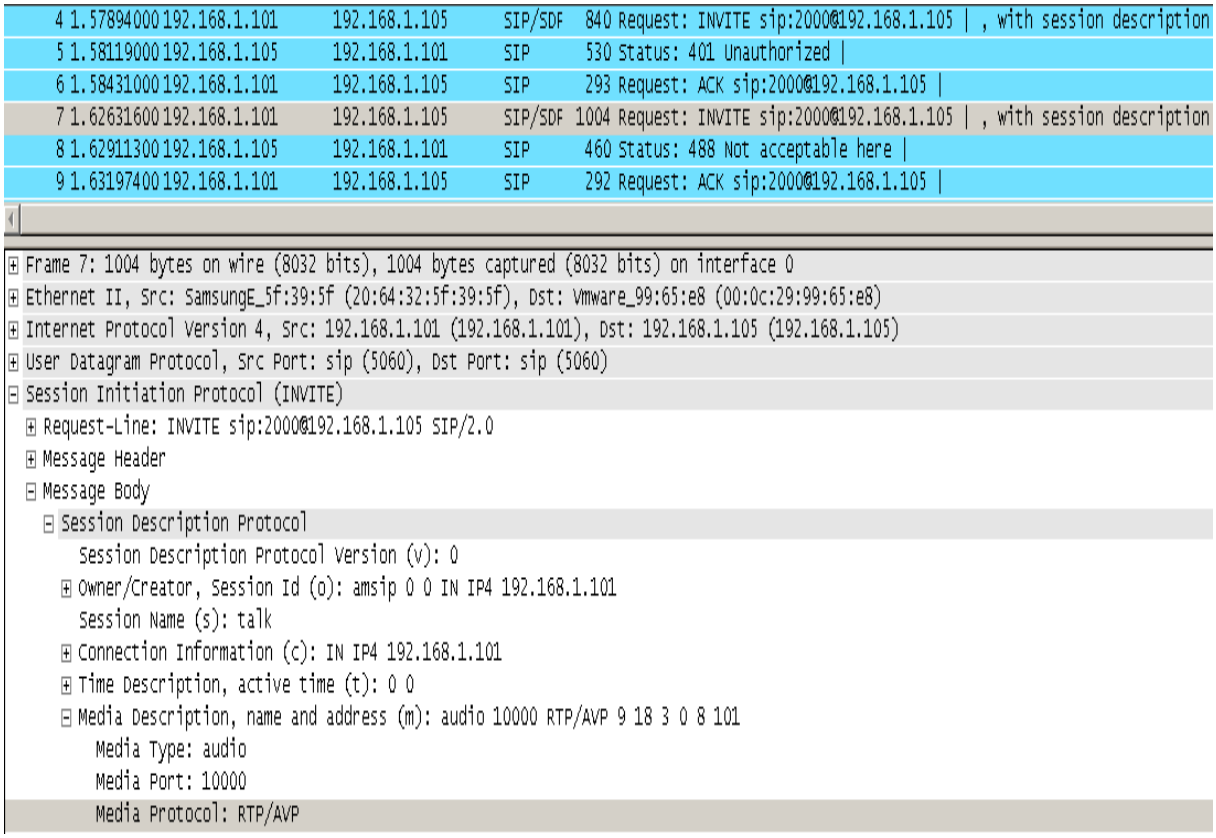


Obr. 4.7 – Zachycená komunikace Wiresharkem při snaze navázat komunikaci SIP softwarového klienta Media5-fone s ostatními SIP softwarovými klienty.

Dalším klientem, kterému se nepovedlo komunikovat na protokolu SRTP je SIP softwarový klient is-Phone. Jeho snaha o komunikaci na protokolu SRTP je zachycena pomocí Wiresharku na obr. č. 4.9. Na obr. 4.8 je uvedeno varování tel. ústředny Asterisk při snaze o navázání spojení SIP softwarového klienta is-Phone bez protokolu SRTP i když byl v jeho vlastním menu nastaven.



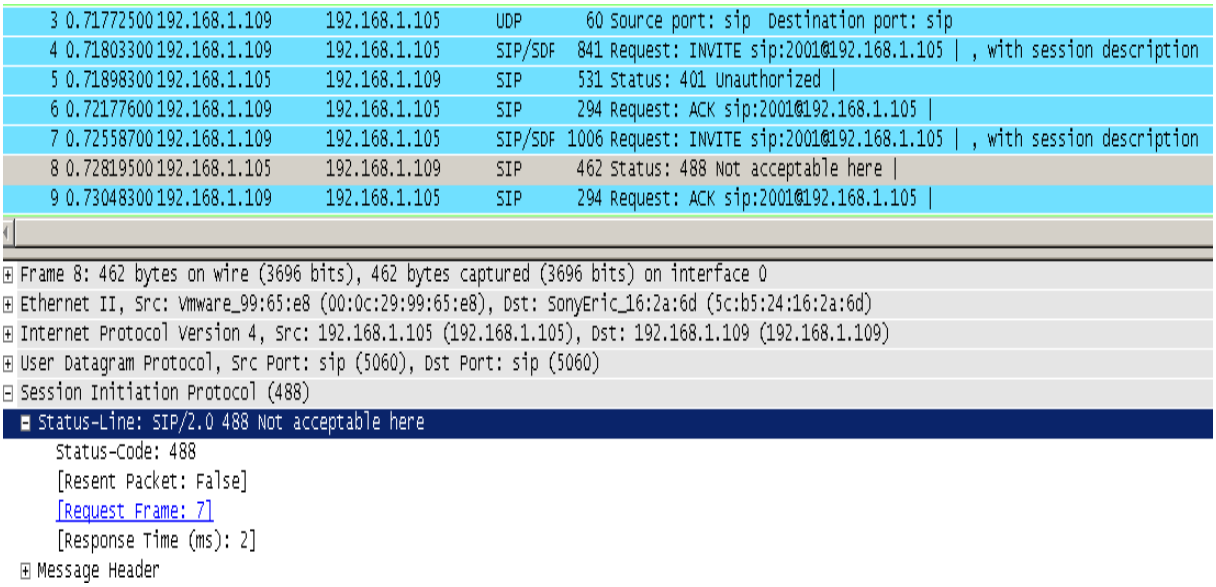
Obr. 4.8 Varovné hlášení Asterisku.



Obr. 4.9 – Zachycení zprávy INVITE SIP klienta is-Phone na tel. ústřednu Asterisk.

Na obr. 4.9 je vidět, že v SIP zprávě INVITE klienta is-Phone na IP adrese 192.168.1.101 směřující na tel. ústřednu Asterisk na IP adrese 192.168.1.105 je v přenášeném protokolu SDP záznam RTP/AVP. To znamená, že žádost INVITE SIP klienta obsahuje žádost o navázání spojení na protokolu RTP a ne na protokolu SRTP. Kdyby byla snaha o navázání komunikace SIP klienta na protokolu SRTP, obsahoval by záznam Media Protocol: RTP/SAVP (Secure Audio and Video).

Dále bylo prováděno zjištění důvodu varování u SIP klienta is-Phone, kdy ve Wiresharku po odchycení paketu na řádku 8 bylo zjištěno, že se jedná o chybové hlášení protokolu SIP s číslem 488 – Not accetable here, čímž bylo SIP klientovi sděleno, že jeho žádosti o spojení bez protokolu SRTP nebylo vyhověno. Klient se tedy nedohodnul pomocí protokolu SDP na podmínkách spojení. Toto je uvedeno na obr. 4.10.



Obr. 4.10 Odchycení paketu ve Wiresharku při snaze navázat komunikaci softwarového klienta is-Phone na protokolu SRTP.

Při tomto testování bylo nastaveno v sekci `[general]` v konfiguračním souboru *sip.conf* telefonní ústředny Asterisk `srtpcapable=yes`, tzn. nutná podmínka pro úspěšné spojení je, že RTP pakety budou šifrovány. Asteriskem však bylo oznámeno varování uvedené na obr. 4.8 vždy, když volajícím byl SIP softwarový klient is-Phone. Tímto varováním Asterisk dával na vědomí, že se SIP klient nesnaží zahájit šifrovanou komunikaci. Asterisk tedy zamítl zahájení nešifrovaného přenosu RTP dat.

Z obr. 4.10 je také vidět na komunikaci mezi SIP klientem is-Phone na IP adrese 192.168.1.109 a tel. ústřednou Asterisk na IP adrese 192.168.1.105 jejich vzájemná komunikace s nezabezpečenou SIP signalizací. Kdyby tedy nebyla na telefonní ústředně nastavena podmínka `srtpcapable=yes`, došlo by ke spojení a vzájemné komunikaci SIP softwarových klientů nešifrovanými RTP pakety. Následně by byla vzájemná komunikace pomocí Wiresharku snadno odchycena, zpracována a přehrána - odposlechnuta. Tímto lze ukázat, že i nastavení podmínek zabezpečení na straně telefonní ústředny má své opodstatnění.

4.3.1.3 Testování SIP softwarových klientů s aktivním šifrováním RTP paketů pomocí SRTP a šifrováním SIP signalizace pomocí TLS mezi SIP softwarovými klienty prostřednictvím tel. ústředny Asterisk

Do tohoto testování byli zahrnuti všichni SIP softwaroví klienti na operačním systému Android, kteří byli vyhledáni a současně podporují komunikaci na protokolu TLS i SRTP. Jedná se o SIP softwarové klienty: CSipSimple, Groundwire, AcrobitsSoftphone, COCOS VoIP, Media5-fone, Voip by antisip, Bria, iPhytter, is-Phone.

V následující tabulce č. 4.4 jsou uvedeny výsledky testování, kde je uvedeno, kteří SIP klienti na těchto dvou protokolech úspěšně dohodnou podmínky spojení a následně zrealizují datový přenos.

Úspěšnost navázání komunikace SIP klient – Asterisk – SIP klient na protokolech TLS i SRTP									
Volající	Volaný								
	CSip Simple	**COCOS VoIP**	**Ground-wire**	**Acrobits Softphone**	**Media5-fone**	**Voip by antisip**	**Bria**	**iPhytter**	**is-Phone**
CSipSimple	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
COCOS VoIP	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Groundwire	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Acrobits Softphone	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Media5-fone	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne
Voip by antisip	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
Bria	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
iPhytter	Ne	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ano
is-Phone	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Ne

Tabulka 4.4 – Výsledky testování SIP softwarových klientů na protokolech TLS a SRTP při navazování spojení mezi sebou navzájem prostřednictvím tel. ústředny Asterisk

Při snaze o vyjednání spojení SIP softwarových klientů COCOS VoIP, Groundwire, AcrobitsSoftphone, Media5-fone, Voip by antisip, Bria, iPhytter se SIP klientem CSipSimple telefonní ústředna Asterisk oznamovala následující varování uvedené na obr. 4.11:

```
SSL certificate ok
  == Problem setting up ssl connection: error:14094410:lib(20):SSL3_READ_BYTES:sslv3 alert handshake failure
                WARNING[2563]: tcptls.c:261 handle_tcptls_connection: FILE * open failed!
```

Obr. 4.11 Varování Asterisku při snaze o navázání vzájemné komunikace SIP softwarových klientů na protokolech TLS a SRTP.

Následná analýza ve Wiresharku byla shodná se zachycenou analýzou uvedenou na obr. 4.5. Nebyly tedy vyjednány podmínky spojení s CSipSimple, nebo Bria z důvodu snahy komunikovat pomocí protokolu SSLv3 a ne pomocí protokolu TLS, nebo z důvodu nedodržení RFC doporučení u protokolu TLS.

Jiné varování oznamující Asterisk je při komunikaci SIP softwarového klienta Media5-fone a mezi ostatními SIP softwarovými klienty uvedeného na obr. 4.12. Při tomto testování se však Asterisk omezil jen na varování oproti testování bez zabezpečené SIP signalizace na protokolu TLS, kde toto varování rozšířil i o další oznámení, které je zachyceno na obr. 4.6. v kapitole 4.3.1.2.

```
WARNING[3119][C-0000000e]: chan_sip.c:10427 process_sdp: Can't provide secure audio requested in SDP offer
```

Obr. 4.12 Varovné hlášení Asterisku při snaze navázat komunikaci SIP klienta Media5-fone.

Zachycenou komunikací ve Wiresharku toho ale z důvodu probíhající zabezpečené komunikace nelze moc zjistit, viz obr. 4.13.

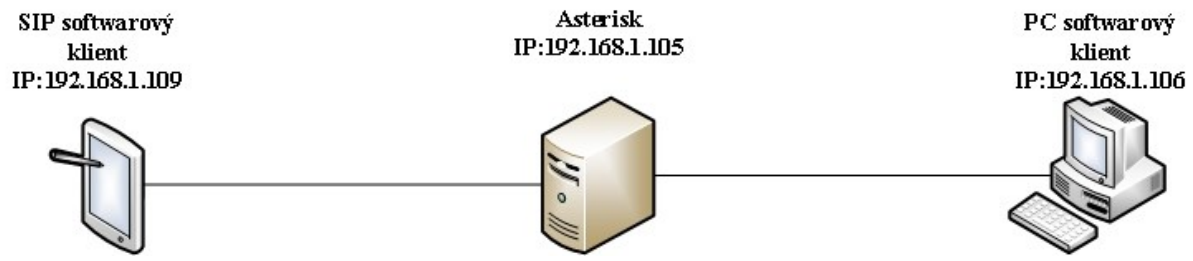
4	1.23301900	192.168.1.109	192.168.1.105	TLSv1 1287 Application Data
5	1.23489100	192.168.1.105	192.168.1.109	TLSv1 652 Application Data, Application Data
6	1.44134200	192.168.1.105	192.168.1.109	TLSv1 652 [TCP Retransmission] Application Data, Application Data
7	1.44259400	192.168.1.109	192.168.1.105	TLSv1 1287 [TCP Retransmission] Application Data
8	1.44287600	192.168.1.105	192.168.1.109	TCP 78 [TCP Dup ACK 6#1] sip-tls > i-net-2000-npr [ACK] Seq=587 Ack=1222 Win=244 Len=0 TSval=2377
9	1.75801500	192.168.1.109	192.168.1.105	TCP 66 i-net-2000-npr > sip-tls [ACK] Seq=1222 Ack=587 Win=408 Len=0 TSval=1616568 TSecr=2376967
10	1.75870400	192.168.1.109	192.168.1.105	TCP 78 [TCP Dup ACK 9#1] i-net-2000-npr > sip-tls [ACK] Seq=1222 Ack=587 Win=408 Len=0 TSval=1616
11	1.76210800	192.168.1.109	192.168.1.105	TLSv1 439 Application Data
12	1.76245700	192.168.1.105	192.168.1.109	TCP 66 sip-tls > i-net-2000-npr [ACK] Seq=587 Ack=1595 Win=282 Len=0 TSval=2377099 TSecr=1616569
13	1.76507200	192.168.1.109	192.168.1.105	TLSv1 1447 Application Data
14	1.76545500	192.168.1.105	192.168.1.109	TCP 66 sip-tls > i-net-2000-npr [ACK] Seq=587 Ack=2976 Win=327 Len=0 TSval=2377100 TSecr=1616569
15	1.76872900	192.168.1.105	192.168.1.109	TLSv1 588 Application Data, Application Data
16	1.77660300	192.168.1.109	192.168.1.105	TLSv1 439 Application Data
17	1.83132200	192.168.1.105	192.168.1.109	TCP 66 sip-tls > i-net-2000-npr [ACK] Seq=1109 Ack=3349 Win=370 Len=0 TSval=2377116 TSecr=1616570

Obr. 4.13 Zachycená komunikace mezi SIP klienty Media5-fone a tel. ústřednou Asterisk při snaze navázat spojení s ostatními SIP klienty.

Z této komunikace lze zjistit, že SIP klient Media5-fone na IP adrese 192.168.1.109 nedokáže vyjednat spojení s telefonní útřednou Asterisk na IP adrese 192.168.1.105. Tato informace ve spojení s varováním Asterisku dokazuje, že žádosti o vyjednání podmínek spojení nebylo vyhověno z důvodu, že Asterisk komunikaci na protokolu SRTP, který nese protokol SDP, zamítnul. Stejná situace nastala i při testování SIP klienta is-Phone. Důvody neuskutečnění komunikace SIP klientů is-Phone a Media5-fone jsou rozebrány v kapitole 4.3.1.2.

4.3.2 Testování zabezpečené komunikace SIP klient – Asterisk – PC klient

Při tomto testování bude uvedeno, jak úspěšné je navázání komunikace mezi SIP softwarovými klienty nainstalovanými na operačním systému Android a PC softwarovým klientem s šifrováním SIP signalizace protokolem TLS, s aktivním šifrováním RTP paketů protokolem SRTP, s aktivním šifrováním RTP paketů protokolem ZRTP, s šifrováním SIP signalizace protokolem TLS spolu s aktivním šifrováním RTP paketů na protokolu SRTP. Schéma zapojení je uvedeno na obr. 4.14.



Obr. 4.14 Schéma zapojení při testování SIP softwarový klient – Asterisk – PC klient (OS Windows).

4.3.2.1 Testování SIP softwarových klientů s šifrováním SIP signalizace pomocí TLS mezi SIP softwarovými klienty Android a PC softwarovým klientem na OS Windows prostřednictvím tel. ústředny Asterisk

Při tomto testování všichni SIP softwaroví klienti nainstalovaní na operačním systému Android úspěšně vyjednali podmínky spojení a následnou úspěšnou komunikaci, ať už byli v roli volaného nebo volajícího.

4.3.2.2 Testování SIP softwarových klientů s aktivním šifrováním RTP paketů pomocí SRTP mezi SIP softwarovými klienty Android a PC softwarovým klientem na OS Windows prostřednictvím tel. ústředny Asterisk

Toto testování mělo stejný výsledek, jako testování uvedené v kapitole 4.3.2.4. Tzn. že vyjma snahy o navázání spojení SIP klienta is-Phone v roli volajícího se všem klientům, buď v roli volaného nebo volajícího podařilo na protokolu SRTP komunikovat.

U SIP klienta is-Phone byla provedena analýza důvodu, proč nelze navázat spojení v případě, kdy byl volajícím. Tato analýza měla stejný výsledek, jako analýza uvedená v kapitole 4.3.1.2. na obr. 4.9, 4.10 (výpisy zachycené komunikace z Wiresharku). Asterisk tedy oznámil varování, že očekával spojení na protokolu SRTP a bez komunikace na tomto protokolu spojení neučiní. Viz obr. 8 (varování Asterisku). Nebyly dohodnuty pomocí protokolu SDP podmínky spojení a hovor byl ukončen.

4.3.2.3 Testování SIP softwarových klientů s aktivním šifrováním RTP paketů pomocí ZRTP mezi SIP softwarovými klienty Android a PC softwarovým klientem na OS Windows prostřednictvím tel. ústředny Asterisk

Do testování byli zařazeni klienti, kteří dokáží navázat spojení na protokolu ZRTP. Jedná se o SIP softwarové klienty: CSipSimple, Groundwire, AcrobitsSoftphone, MizuDroid a PC softwarový klient na OS Win7 PhonerLite. Tento byl do testování zařazen pouze z důvodu komplexnosti testování. MizuDroid, GroundWire a AcrobitsSoftphone nebyl testován na odchozí hovory z důvodu, že tato možnost vytvoření spojení na protokolu ZRTP je placená.

Úspěšnost navázání komunikace SIP klient – Asterisk – SIP klient na protokolu ZRTP					
Volající	Volaný				
	CSipSimple	**Ground-wire**	**Acrobits Softphone**	**MizuDroid**	**PhonerLite**
CSipSimple	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**
Groundwire	**Netestováno**	**Netestováno**	**Netestováno**	**Netestováno**	**Netestováno**
Acrobits Softphone	**Netestováno**	**Netestováno**	**Netestováno**	**Netestováno**	**Netestováno**
MizuDroid	**Netestováno**	**Netestováno**	**Netestováno**	**Netestováno**	**Netestováno**
PhonerLite	**Ano**	**Ano**	**Ano**	**Ano**	**Ano**

Tabulka č. 4.5 – Úspěšnost navázání spojení SIP softwarových klientů na protokolu ZRTP.

Jak bylo uvedeno výše, protokol ZRTP hlavně slouží k počátečnímu vytvoření spojení za účelem bezpečného přenosu řetězce k výpočtu Master Key. Tzn. že případný útočník může zjistit kdo koho volá, ale samotnou komunikaci neodposlechne.

4.3.2.4 Testování SIP softwarových klientů s aktivním šifrováním RTP paketů pomocí SRTP a šifrováním SIP signalizace pomocí TLS mezi SIP softwarovými klienty Android a PC softwarovým klientem na OS Windows prostřednictvím tel. ústředny Asterisk

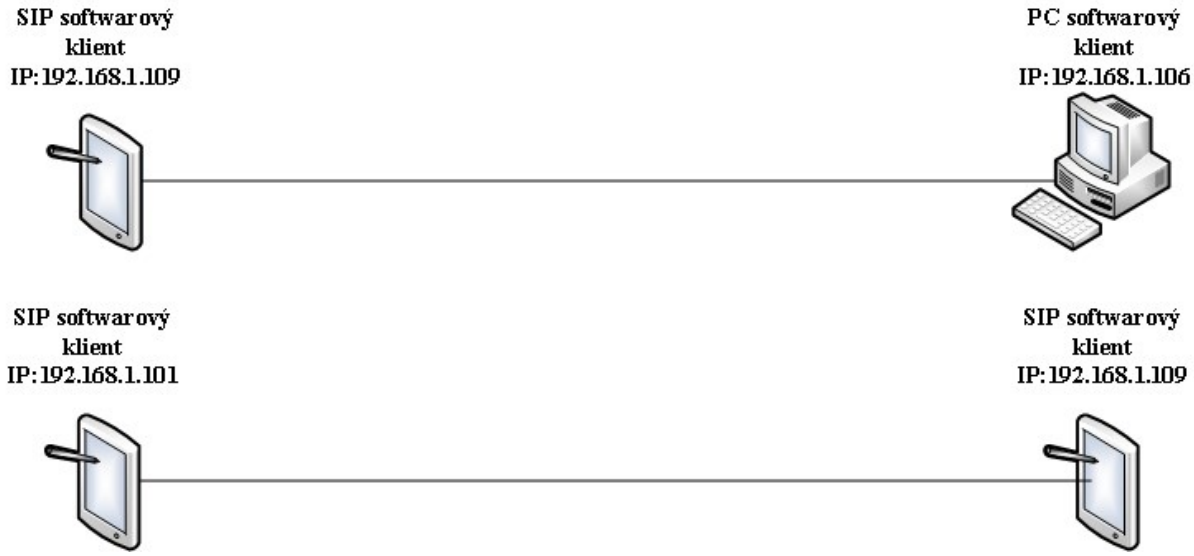
Do tohoto testování byli zahrnuti všichni SIP softwaroví klienti na operačním systému Android, kteří byli testování již v kapitole 4.3.1. a současně podporují komunikaci na protokolu TLS i SRTP. Jedná se o SIP softwarové klienty: CSipSimple, Groundwire, AcrobitsSoftphone, COCOS VoIP, Media5-fone, Voip by antisip, Bria, iPhytter, is-Phone. Jako softwarový klient byl v této části použit klient PhonerLite nainstalovaný na operačním systému Windows 7 proffesional.

Při tomto testování probíhala zabezpečená komunikace vyjma SIP klienta is-Phone úspěšně. Bylo testováno volání PC SIP klienta PhonerLite na SIP klienta a opačně, tj. že všichni SIP softwaroví klienti byli volajícími i volanými.

U SIP klienta is-Phone byla provedena analýza důvodu, proč nelze navázat spojení v případě, kdy byl volajícím. V případě, že byl is-Phone volaným bylo spojení navázáno. V případě, že byl
is-Phone volajícím, Asterisk oznámil varování, že očekával spojení na protokolu SRTP a bez komunikace na tomto protokolu spojení neučiní. Viz obr. 4.12. Výsledky analýzy ve Wiresharku jsou rovněž obdobné, těm, které byly uvedeny v kapitole 4.3.1.3. Tzn., že komunikace probíhala stejně, jak je uvedeno na obr. 4.13 ve výpisu z Wiresharku. Nebyly dohodnuty pomocí protokolu SDP podmínky spojení a hovor byl ukončen.

4.3.3 Testování zabezpečené komunikace SIP klient – SIP klient na OS Android

Při tomto testování byla přímo z jednotlivých SIP softwarových klientů volána adresa sip adresa ve tvaru *uživatelské jméno@IP adresa volaného* s přednadstavenými podmínkami spojení u jednotlivých SIP klientů (např. současné použití protokolu TLS i SRTP). Do testování byli opět zahrnuti SIP klienti: CSipSimple, Groundwire, AcrobitsSoftphone, COCOS VoIP, Media5-fone, Voip by antisip, Bria, iPhytter, is-Phone a také SIP klient na OS Windows 7 Linphone. Schéma zapojení je uvedeno na obr. 4.15.



Obr. 4.15 – Schéma zapojení při testování SIP softwarový klient – SIP softwarový klient.

4.3.3.1 Testování SIP softwarových klientů s šifrováním SIP signalizace pomocí TLS mezi SIP softwarovými klienty Android a PC softwarovým klientem na OS Windows navzájem

Při tomto testování byla u jednotlivých SIP softwarových klientů v jejich vlastním menu nastavena podmínka komunikace na protokolu TLS. Výsledky testování jsou uvedeny v tabulce 4.6a, 4.6b.

Úspěšnost navázání komunikace SIP klient – SIP klient na protokolu TLS					
Volající	Volaný				
	CSipSimple	**COCOS VoIP**	**Groundwire**	**Acrobits Softphone**	**Media5-fone**
CSipSimple	**Ano**	**Ne**	**Ne**	**Ne**	**Ne**
COCOS VoIP	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Groundwire	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Acrobits Softphone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Media5-fone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Voip by antisip	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Bria	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
iPhytter	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
is-Phone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
PC klient Linphone	**Ano**	**Ne**	**Ne**	**Ne**	**Ne**

Tabulka 4.6a – Výsledky úspěšnosti o navázání spojení mezi SIP softwarovými klienty při testování s podmínkou spojení na protokolu TLS.

Úspěšnost navázání komunikace SIP klient – Android – SIP klient na protokolu TLS					
Volající	Volaný				
	Voip by antisip	**Bria**	**iPhytter**	**is-Phone**	**PC klient Linphone**
CSipSimple	**Ano**	**Ne**	**Ne**	**Ne**	**Ano**
COCOS VoIP	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Groundwire	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Acrobits Softphone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Media5-fone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Voip by antisip	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Bria	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
iPhytter	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
is-Phone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
PC klient Linphone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**

Tabulka 4.6b – Výsledky úspěšnosti o navázání spojení mezi SIP softwarovými klienty při testování s podmínkou spojení na protokolu TLS.

Jak je z tabulky vidět, tak úspěšnost tohoto testování je mizivá. Jediný softwarový klient, na OS Android, CSipSimple dokázal zprostředkovat zabezpečenou komunikaci a to jen mezi SIP klienty CSipSimple a v případě, že byl CSipSimple volajícím, tak se SIP klientem, na OS Android, Voip by antisip.

4.3.3.2 Testování SIP softwarových klientů s aktivním šifrováním RTP paketů pomocí SRTP mezi SIP softwarovými klienty Android a PC softwarovým klientem na OS Windows navzájem

Při tomto testování byla u jednotlivých SIP softwarových klientů v jejich vlastním menu nastavena podmínka komunikace na protokolu SRTP. Výsledky testování jsou uvedeny v tabulce 4.7a, 4.7b.

Úspěšnost navázání komunikace SIP klient – SIP klient na protokolu SRTP					
Volající	Volaný				
	CSipSimple	**COCOS VoIP**	**Groundwire**	**Acrobits Softphone**	**Media5-fone**
CSipSimple	Ano	Ano	Ne	Ne	Ne
COCOS VoIP	Ne	Ne	Ne	Ne	Ne
Groundwire	Ne	Ne	Ne	Ne	Ne
Acrobits Softphone	Ne	Ne	Ne	Ne	Ne
Media5-fone	Ne	Ne	Ne	Ne	Ne
Voip by antisip	Ano	Ano	Ano	Ne	Ne
Bria	Ne	Ne	Ne	Ne	Ne
iPhytter	Ne	Ne	Ne	Ne	Ne
is-Phone	Ne	Ano	Ne	Ne	Ne
PC klient Linphone	Ano	Ano	Ne	Ne	Ne

Tabulka 4.7a – Výsledky úspěšnosti o navázání spojení mezi SIP softwarovými klienty při testování s podmínkou spojení na protokolu SRTP.

Úspěšnost navázání komunikace SIP klient – Android – SIP klient na protokolu SRTP					
Volající	Volaný				
	Voip by antisip	**Bria**	**iPhytter**	**is-Phone**	**PC klient Linphone**
CSipSimple	Ano	Ne	Ne	Ne	Ano
COCOS VoIP	Ne	Ne	Ne	Ne	Ne
Groundwire	Ano	Ne	Ne	Ne	Ne
Acrobits Softphone	Ne	Ne	Ne	Ne	Ne
Media5-fone	Ne	Ne	Ne	Ne	Ne
Voip by antisip	Ano	Ne	Ne	Ano	Ano
Bria	Ne	Ne	Ne	Ne	Ne
iPhytter	Ne	Ne	Ne	Ne	Ne
is-Phone	Ne	Ne	Ne	Ano	Ne
PC klient Linphone	Ano	Ne	Ne	Ne	

Tabulka 4.7b – Výsledky úspěšnosti o navázání spojení mezi SIP softwarovými klienty při testování s podmínkou spojení na protokolu SRTP.

4.3.3.3 Testování SIP softwarových klientů s aktivním šifrováním RTP paketů pomocí SRTP a šifrováním SIP signalizace pomocí TLS SIP softwarovými klienty Android a PC softwarovým klientem na OS Windows navzájem

Při tomto testování byly u jednotlivých SIP softwarových klientů v jejich vlastním menu nastaveny podmínky spojení, tzn. že komunikace má probíhat jak na protokolu SRTP, tak na protokolu TLS. Poté byly volány IP adresy s názvem uživatelského jména volané strany. Výsledky testování jsou uvedeny v tabulce 4.8a, 4.8b.

Úspěšnost navázání komunikace SIP klient – SIP klient na protokolu SRTP a TLS					
Volající	Volaný				
	CSipSimple	**COCOS VoIP**	**Groundwire**	**Acrobits Softphone**	**Media5-fone**
CSipSimple	**Ano**	**Ne**	**Ne**	**Ne**	**Ne**
COCOS VoIP	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Groundwire	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Acrobits Softphone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Media5-fone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Voip by antisip	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Bria	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
iPhytter	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
is-Phone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
PC klient Linphone	**Ano**	**Ne**	**Ne**	**Ne**	**Ne**

Tabulka 4.8a – Výsledky úspěšnosti o navázání spojení mezi SIP softwarovými klienty při testování s podmínkou spojení na protokolu SRTP a TLS.

Úspěšnost navázání komunikace SIP klient – Android – SIP klient na protokolu SRTP a TLS					
Volající	Volaný				
	Voip by antisip	**Bria**	**iPhytter**	**is-Phone**	**PC klient Linphone**
CSipSimple	**Ano**	**Ne**	**Ne**	**Ne**	**Ano**
COCOS VoIP	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Groundwire	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Acrobits Softphone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Media5-fone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Voip by antisip	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
Bria	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
iPhytter	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
is-Phone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**
PC klient Linphone	**Ne**	**Ne**	**Ne**	**Ne**	**Ne**

Tabulka 4.8b – Výsledky úspěšnosti o navázání spojení mezi SIP softwarovými klienty při testování s podmínkou spojení na protokolu SRTP a TLS.

5 Nejvhodnější SIP klient a jeho vylepšení z pohledu bezpečnosti

Na začátku testování jsem byl zaskočen tím, že pouze 29% vybraných klientů podporuje šifrování pomocí protokolu TLS a necelých 36% protokol SRTP (tato norma vznikla již v roce 2004). Nativní SIP klient integrovaný v operačním systému Android od verze 2.3 do současné doby (aktuálně verze 4.2.1 – únor 2013) nepodporuje protokol TLS ani protokol SRTP. V průběhu testování bylo zjištěno, že SIP klienti Media5-fone (screenshot obr. 5.1) a is-Phone (screenshot obr. 5.2) nedokáží na protokolu SRTP dohodnout podmínky spojení a SIP klienti CsipSimple a Bria (screenshot obr. 5.3) nedokáží s ostatními SIP klienty na protokolu TLS navázat zabezpečenou komunikaci.

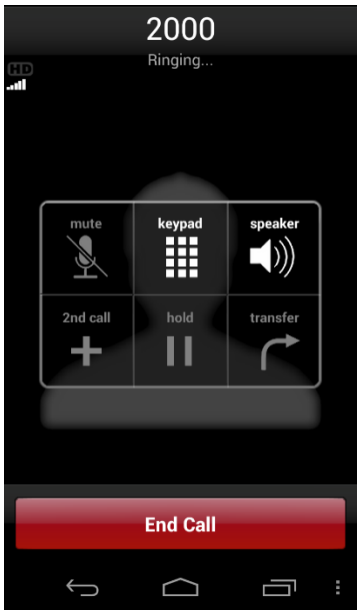
Na druhou stranu lze částečně zjištění o slabé podpoře šifrovacích protokolů zmírnit tím, že první komerční smartphone s OS Android byl dán na trh v říjnu 2008 (leden 2009 v ČR) a RFC pro TLS vznikla v srpnu 2008.

Lze říci, že z volně dostupných SIP softwarových klientů je z pohledu komplexnosti nastavení zabezpečení (TLS, SRTP, ZRTP, možnost vložení vlastních certifikátů) nejvhodnější SIP softwarový klient CSipSimple (screenshot obr. 5.4). U tohoto klienta bych však navrhoval zlepšit komunikaci na protokolu TLS, kdy nebyly dodrženy RFC doporučení pro SIPS, nebo protokol TLS.

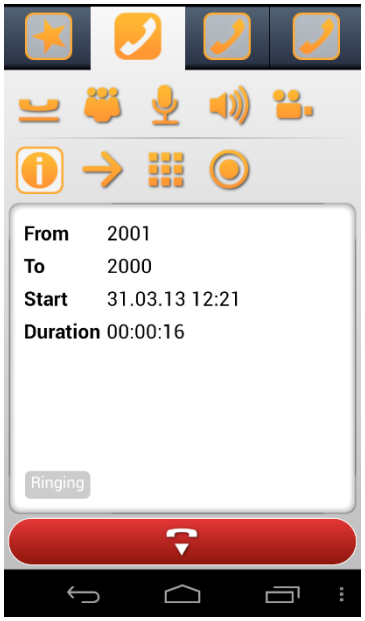
Z placených SIP softwarových klientů je z hlediska zabezpečení a kompatibility k ostatním SIP klientům nejlepší klient Groundwire (screenshot obr. 5.5) a Acrobits Softphone (screenshot obr. 5.6). U těchto klientů bych však navrhoval doimplementovat funkcionalitu pro práci s certifikáty. Dále žádný z testovaných SIP softwarových klientů (vyjma CSipSimple) neoznamoval, že probíhá nebo neprobíhá zabezpečená komunikace na předem nastavených podmínkách spojení. Tato funkcionalita by také byla vhodná doimplementovat.

Na operačním systému Android doposud není žádná externí aplikace typu Zfone [32], která by na protokolu ZRTP šifrovala komunikaci mezi SIP softwarovými klienty, jejíž návrh by umožnil komunikaci na tomto protokolu pro jakéhokoliv SIP klienta.

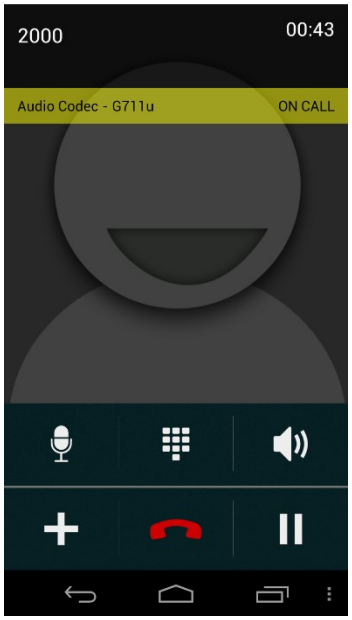
Na obr. 5.7 je v grafu znázorněno procentuální vyjádření dostupných SIP klientů podporujících zabezpečenou komunikaci v různých kombinacích protokolu TLS zabezpečujícím SIP signalizaci s šifrováním RTP paketů pomocí protokolu SRTP nebo ZRTP.



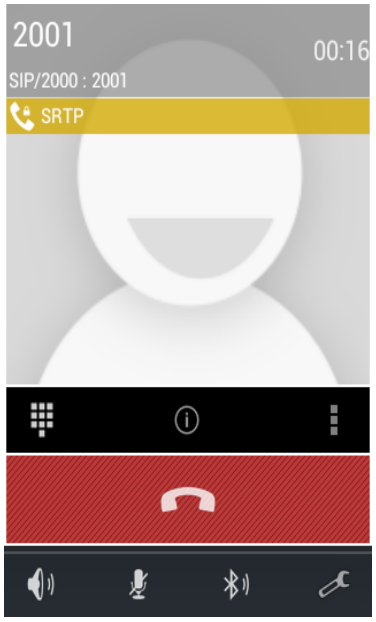
Obr. 5.1 - Screenshot SIP klienta Media5-fone při vytáčení nastaveného účtu s přihlašovacím jménem 2000 v tel. ústředně Asterisk.



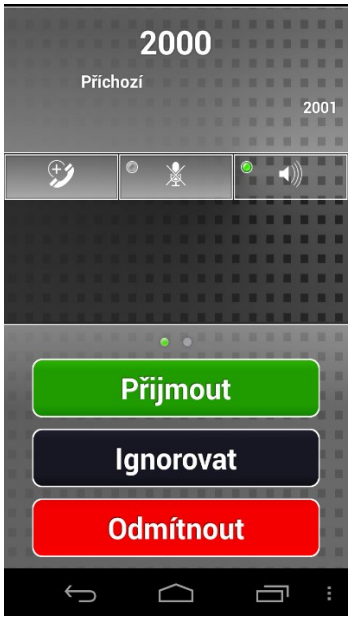
Obr. 5.2 - Screenshot SIP klienta is-Phone při vytáčení účtu 2001, kdy volající účet byl 2001.



Obr. 5.3 - Screenshot SIP klienta Bria při úspěšné komunikaci mezi účty 2000 a 2001 s informací o použitém audio kodeku.

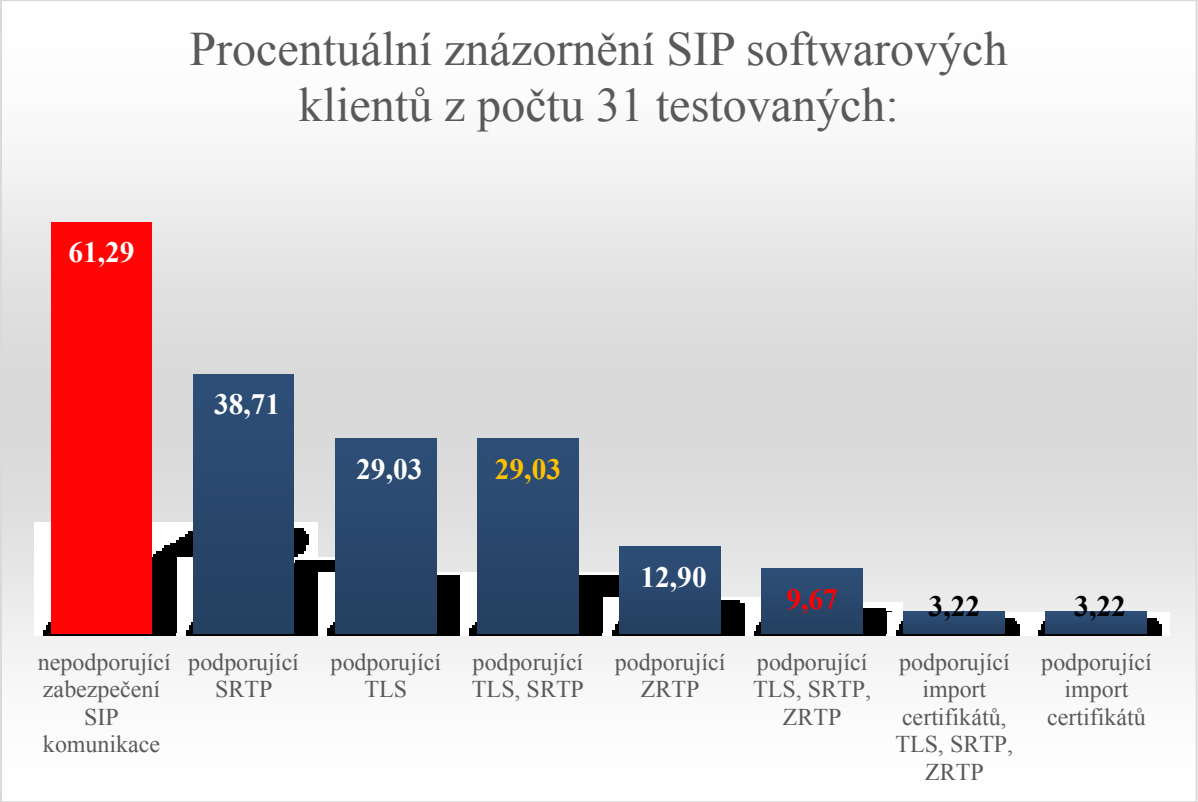


Obr. 5.4 Screenshot SIP klienta CSipSimple při úspěšném navázání komunikace na protokolu SRTP.



Obr. 5.5 - Screenshot SIP klienta Groundwire při oznámení o příchozím hovoru z účtu 2000.

Obr. 5.6 Screenshot klienta AcrobitsSoftphone při úspěšném navázání komunikace s informací o použitém audio kodeku.



Obr.5.7-Graf procentního vyjádření dostupných SIP klientů podporujících zabezpečenou SIP komunikaci.

Jen pro zajímavost zde uvedu ceník SIP softwarových klientů, kteří byli testováni:

Acrobits SoftPhone – 125 Kč, za příplatek 500 Kč podpora protokolu ZRTP pro odchozí hovory,
Bria Android – 183 Kč,
COCOS VoIP – zdarma,
CsipSimple – zdarma,
Groundwire – 179 Kč, za příplatek 500 Kč podpora protokolu ZRTP pro odchozí hovory,
iPhytter – 100 Kč,
is-Phone – 388 Kč,
Media5-fone – zdarma, za příplatek 70 Kč podpora TLS a SRTP,
MizuDroid – zdarma, za příplatek 280 Kč podpora protokolu ZRTP pro odchozí hovory,
VoIP by antisip – zdarma.

6 Závěr

V bakalářské práci jsem se soustředil zmapovat dostupné SIP softwarové klienty na OS Android, kteří jsou nezávislí na předdefinovaných VoIP providerech. Do testu byli zahrnuti SIP softwaroví klienti, kteří jsou dostupní zdarma i ti, kteří jsou zpoplatněni.

Po úvodním seznámením se ze základy způsobu VoIP SIP komunikace a zabezpečením RTP paketů v kapitole 2, byly v následující kapitole uvedeny způsoby zabezpečení přenosu dat. Na podkladě těchto informací byli postupně otestováni SIP softwaroví klienti za účelem zjištění jejich nezávislosti na VoIP providerech a jejich možností nabízené úrovně zabezpečení. Na základě těchto výsledků byli vybráni SIP softwaroví klienti podporující zabezpečení SIP signalizace na protokolu TLS spolu s šifrováním RTP paketů protokolem SRTP, nebo ZRTP. Tito SIP klienti byli následně otestováni, zda skutečně deklarovanou úroveň zabezpečení podporují. Ke zjištění skutečných vlastností z pohledu bezpečnosti při přenosu dat byla použita aplikace Wireshark.

Na základě výsledků testování několika variant zapojení (SIP klient - Asterisk - SIP klient, SIP klient - Asterisk - PC klient, SIP klient - SIP klient) byli v kapitole 5 definováni nejvhodnější SIP softwaroví klienti pro využití v praxi, kteří nabízejí maximální zabezpečení SIP komunikace. V této kapitole jsou také uvedeny návrhy vylepšení vybraných SIP klientů pro jejich maximální úroveň, ať už z pohledu informovanosti uživatele o probíhajícím zabezpečeném přenosu dat nebo z pohledu programátora pro vylepšení, nebo rozšíření šifrovacích algoritmů.

Tato bakalářská práce by měla být čtenáři pomocným vodítkem při vlastním výběru SIP softwarového klienta na platformě Android z pohledu zabezpečení SIP signalizace protokolem TLS a samotného šifrovaného přenosu RTP paketů na protokolu SRTP, nebo ZRTP proti odposlechu.

Literatura

[1] **DDWorld.** Prodeje mobilních telefonů padají – používáme je déle a trhu vládne SAMSUNG a ANDROID. [Online] [Citace 10.3.2013.]. Dostupné z URL: http://www.ddworld.cz/aktuality/notebook-nb/prodeje-mobilnich-telefonu-padaji-pouzivame-je-dele-a-trhu-vladne-samsung-a-android-2.html.

[2] **Strategy Analytics.** Android and Apple iOS Capture a Record 92 Percent Share of Global Smartphone Shipments in Q4 2012. [Online] [Citace 10.3.2013.]. Dostupné z URL: http://blogs.strategyanalytics.com/WSS/post/2013/01/28/Android-and-Apple-iOS-Capture-a-Record-92-Percent-Share-of-Global-Smartphone-Shipments-in-Q4-2012.aspx.

[3] **Venturebeat.** Android captured almost 70% global smartphone market share in 2012, Apple just under 20%. [Online] [Citace 10.3.2013.]. Dostupné z URL: http://venturebeat.com/2013/01/28/android-captured-almost-70-global-smartphone-market-share-in-2012-apple-just-under-20/.

[4] **Forbes.** Samsung Increasing Its Smartphone Market Share vs. Apple and Rest of the Pack. [Online] [Citace 8.2.2013]. Dostupné z URL: http://www.forbes.com/sites/chuckjones/2013/01/25/samsung-increasing-its-smartphone-market-share-vs-apple-and-the-rest-of-the-pack/.

[5] **J. Postel.** RFC 768 – user datagram protocol. Technical report, IETF, 1980.

[6] **H.Schulzrine, S. Casner, R. Frederick, V. Jacobson.** RFC 1889 – a transport protocol for real-time pplications. Technical report, IETF, 1996.

[7] **H.Schulzrine, S. Casner, R. Frederick, V. Jacobson.** RFC 3550 – a transport protocol for real-time pplications. Technical report, IETF, 2003.

[8] **J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler.** RFC 3261 – sip: Session initiation protocol. Technical report, IETF, 2002.

[9] **R. Sparks.** RFC 3515 – The Session Initiation Protocol (SIP) Refer Method, IETF, 2003. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc3515.txt.

[10] **A. B. Roach.** RFC 3265 – Session Initiation Protocol (SIP) – Specific Event Notification, IETF, 2002. Doument dostupný na URL: http://www.ietf.org/rfc/rfc3265.txt.

[11] **K. Morneault, R. Dantu, G. Sidebottom, B. Bidulock, J. Heitz** RFC 3331 – Signaling System 7 (SS7) Message Transfer Part 2 (MTP2): User Adaptation Layer, IETF, 2002. Dokument dostupný z URL: http://tools.ietf.org/rfc/rfc3331.txt.

[12] **S. Donovan**. RFC 2976 – The SIP INFO Method, IETF, 2000. Dokument dostupný z URL: http://www.ietf.org/rfc/rfc2976.txt.

[13] **J. Rosenberg, H. Schulzrine.** – Reliability of Provisional Responses in the Session Initiationn Protocol (SIP), IETF, 2002. Dokument dostupný z URL: http://www.ietf.org/rfc/rfc3262.txt

[14] **B. Cambell, J. Rosenberg, H. Schulzrine, C. Huitema, D. Gurle.** – Session Initiation Protocol (SIP) Extension for Instant Messaging, IETF, 2002. Dokument dostupný z URL: http://www.ietf.org/rfc/rfc3428.txt.

[15] **SIP. CESNET. IPTelWiki:** SIP [Online]. [Citace 8.1.2013]. Dostupné z URL: https://sip.cesnet.cz/cs/protokoly/sip.

[16] **Miroslav Vozňák. –**TECHNICKÉ PRINCIPY IP TELEFONIE. Teorie a praxe IP telefonie [Online]. 2004 [Citace 18.12.2012]. Dokument dostupný z URL: http://www.ip-telefon.cz/archiv/dok_osta/ipt-2004_Principy_IPtel.pdf.

[17] **Miroslav Vozňák.** – Voice over IP. 1. vyd. Ostrava: VŠB-TU Ostrava, 2008. 176 p. ISBN 978-80-248-1828-3.

[18] **M. Handley, V. Jacobson, C. Perkins.** – SDP: Session Description Protocol, IETF, 2006. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc4566.txt

[19] **Wikimedia Foundation.** Wikipedia, the free encyclopedia. [Online]. [Citace 5.1.2013]. Dostupné z URL: http://www.wikipedia.org , duben 2009.

[20] **T. Dierks, E. Rescorla.** – The Transport Layer Security (TLS) Protocol, IETF, 2008. Dostupné z URL: http://www.ietf.org/rfc/rfc5246.txt.

[21] **Dr. Dorgham Sisalem**. SIP security. Chichester, U.K.: Wiley, 2009, xiv, 336 p. ISBN 04-705-1636-4.

[22] **E. Rescorla, N. Modadugu.** – Datagram Transport Layer Security, IETF, 2006. Dokument dostupný na URL: http://tools.ietf.org/html/rfc4347.

[23] **M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman.** RFC 3711 – The Secure Real-time Transport Protocol (SRTP), IETF, 2004.

[24] **P. Zimmermann, A. Johnston, Ed. Avaya, J. Callas** RFC 6189 – ZRTP: Media Path Key Agreement for Unicast Secure RTP, IETF, 2011. Dokument dostupný na URL: http://tools.ietf.org/html/rfc6189.

[25] **E. Rescorla.** RFC 2631 – Diffie-Hellman Key Agrement Method, IETF, 1999. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc2631.txt

[26] **P. Zimmermann, A. Johnston, J.Callas.** ZRTP: Media Path Key Agreement for Secure RTP. Dokument dostupný na URL: http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-15, 2009.

[27] **Ing. Filip Řezáč.** Bezpečnost v IP telefonii. Ostrava, 2011.

[28] **Wireshark.** Dostupné z URL: http://www.wireshark.org/about.html.

[29] **Global Mobile Awards 2013.** Dostupné z URL: http://www.globalmobileawards.com/awards-2013/winners-2012.

[30] **Samsung Galaxy Nexus.** [Online]. [Citace 2.2.2013]. Dostupné z URL: http://www.samsung.com/cz/support/model/GT-I9250TSAXEZ-techspecs.

[31] **SonyEricsson ST15i.** [Online] [Citace 2.2.2013]. Dostupné z URL: http://www.sonymobile.com/gb/products/phones/xperia-mini/specifications.

[32] **Zfone.** [Online] [Citace 1.4.2013]. Dostupné z URL: http://zfoneproject.com/

Adresářová struktura přiloženého DVD

/Android/Aplikace	Soubory *.apk* testovaných SIP softwarových klientů pro OS Android
/Linux/Asterisk	Adresář obsahuje komprimované soubory telefonní ústředny Asterisk a knihovny Asterisku
/Linux/Certifikáty	Adresář obsahuje certifikáty vygenerované Asteriskem, které byly použity při testování
/Linux/Wireshark	Komprimovaný soubor aplikace Wireshark pro OS Linux Ubuntu 32-bit
/Windows/Aplikace	Adresář obsahuje SIP softwarové klienty pro OS Windows 7 využité při testování
/Windows/Wireshark	Komprimovaný soubor aplikace Wireshark pro OS Windows 7 64-bit